

Från: [Maria Solberg](#) för [FI OFA DOF](#)
Till: [Maria Solberg](#)
Kopia: betankande@elanders.com
Ärende: Remiss av SOU 2024:45 Kompletterande bestämmelser till EU:s reviderade förordning om elektronisk identifiering - Svar senast 1/11 2024
Datum: den 1 juli 2024 09:32:08
Bilagor: [Remissmissiv.pdf](#)

Du får inte e-post ofta från fi.ofa.dof@regeringskansliet.se. [Se varför det här är viktigt.](#)

SOU 2024:45 [Kompletterande bestämmelser till EU:s reviderade förordning om elektronisk identifiering](#)

Slutbetänkande Kompletterande bestämmelser till EU:s reviderade förordning om elektronisk identifiering (SOU 2024:45)

Remissinstanser

1. Alvesta kommun
2. Arbetsförmedlingen
3. Bolagsverket
4. Brottsförebyggande rådet
5. Brottsoffermyndigheten
6. Båstads kommun
7. Centrala studiestödsnämnden
8. CGI Sverige AB
9. Chalmers tekniska högskola AB
10. Comfact AB
11. Cybercom Group AB
12. Domstolsverket
13. E-hälsomyndigheten
14. Ekerö kommun
15. Ekobrottsmyndigheten
16. Ekonomistyrningsverket
17. Eskilstuna kommun
18. Finansiell ID-Teknik BID AB
19. Finansinspektionen
20. Fintech Sverige
21. Freja eID Group AB
22. Friskolornas riksförbund
23. Funktionsrätt Sverige
24. Färgelanda kommun
25. Företagarna
26. Försvarets materielverk
27. Försvarets radioanstalt
28. Försvarmakten
29. Försäkringskassan

30. Förvaltningsrätten i Härnösand
31. Förvaltningsrätten i Stockholm
32. Göteborgs kommun
33. Heby kommun
34. Hofors kommun
35. Idéburna skolors riksförbund
36. Ideella Föreningen Teknikföretagen i Sverige
37. IIS – Internetstiftelsen i Sverige
38. Inera AB
39. Inspektionen för arbetslöshetsförsäkringen
40. Integritetsskyddsmyndigheten
41. Kalmar kommun
42. Kammarkollegiet
43. Kammarrätten i Stockholm
44. Knowit AB
45. Kommerskollegium
46. Konkurrensverket
47. Kriminalvården
48. Kungl. Tekniska högskolan
49. Kungsbacka kommun
50. Landsorganisationen i Sverige
51. Lantmäteriet
52. Linköpings kommun
53. Luleå kommun
54. Lunds kommun
55. Lunds Tingsrätt
56. Länsstyrelsen i Blekinge län
57. Länsstyrelsen i Gävleborgs län
58. Länsstyrelsen Norrbottens län
59. Länsstyrelsen i Skåne län
60. Länsstyrelsen i Stockholms län
61. Länsstyrelsen i Uppsala län
62. Länsstyrelsen i Västra Götalands län
63. Malmö kommun
64. Myndigheten för delaktighet
65. Myndigheten för digital förvaltning
66. Myndigheten för samhällsskydd och beredskap
67. Mölndals kommun
68. Nybro kommun
69. Pensionsmyndigheten
70. Polismyndigheten
71. Post- och telestyrelsen

72. Regelrådet
73. Region Dalarna
74. Region Norbotten
75. Riksarkivet
76. Riksbanken
77. Riksdagens ombudsmän
78. Robertsfors kommun
79. Scrive AB
80. Signicat AB
81. Skatteverket
82. Skövde kommun
83. Socialstyrelsen
84. Statens servicecenter
85. Statens skolverk
86. Statistiska centralbyrån
87. Statskontoret
88. Stockholms kommun
89. Storumans kommun
90. Strömstads kommun
91. Svensk e-identitet
92. Svenska bankföreningen
93. Svenskt Näringsliv
94. Sveriges advokatsamfund
95. Sveriges akademikers centralorganisation
96. Sveriges a-kassor
97. Sveriges ambassad i Berlin
98. Sveriges ambassad i London
99. Sveriges Kommuner och Regioner
100. Swedac
101. Swedish FinTech Association
102. Säkerhets- och försvarsföretagen
103. Säkerhetspolisen
104. TechSweden
105. Teknikföretagen
106. Telia AB
107. Tillväxtverket
108. Torsby kommun
109. Trafikverket
110. Tranemo kommun
111. Transportstyrelsen
112. Tranås kommun
113. Umeå universitet

114. Verket för innovationssystem
115. Vetenskapsrådet
116. Värnamo kommun
117. Västra Götalandsregionen
118. Ydre kommun
119. ZealiD AB
120. Åklagarmyndigheten
121. Älvsbyns kommun
122. Örnsköldsviks kommun
123. Östersunds kommun
124. Överkalix kommun

Remissvaren ska ha kommit in till Finansdepartementet **senast den 1 november 2024**. Svaren bör lämnas per e-post till fi.remissvar@regeringskansliet.se och med kopia till fi.ofa.dof.remissor@regeringskansliet.se. Ange diarienummer Fi2024/01413 och remissinstansens namn i ämnesraden på e-postmeddelandet.

Svaret bör lämnas i två versioner: den ena i ett bearbetningsbart format (t.ex. Word), den andra i ett format (t.ex. pdf) som följer tillgänglighetskraven enligt lagen (2018:1937) om tillgänglighet till digital offentlig service. Remissinstansens namn ska anges i namnet på respektive dokument.

Remissvaren kommer att publiceras på regeringens webbplats.

I remissen ligger att regeringen vill ha synpunkter på förslagen eller materialet i betänkandet. Det är endast förslagen och materialet i själva betänkandet som remitteras och inte den externa rapport som kartlägger vissa kostnader som följer direkt av förordningen.

Myndigheter under regeringen är skyldiga att svara på remissen. En myndighet avgör dock på eget ansvar om den har några synpunkter att redovisa i ett svar. Om myndigheten inte har några synpunkter, räcker det att svaret ger besked om detta.

För **andra remissinstanser** innebär remissen en inbjudan att lämna synpunkter.

Betänkandet kan laddas ned från Regeringskansliets webbplats www.regeringen.se.

Remissinstanserna kan utan kostnad beställa tryckta exemplar av betänkandet via ett [beställningsformulär hos Elanders Sverige AB](#).

Råd om hur remissyttranden utformas finns i Statsrådsberedningens promemoria [Svara på remiss \(SB PM 2021:1\)](#). Den kan laddas ned från Regeringskansliets webbplats www.regeringen.se.

Johan Ndure
Departementsråd

Kopia till

Elanders Sverige AB, e-postadress: betankande@elanders.com



Finansdepartementet

Slutbetänkande Kompletterande bestämmelser till EU:s
reviderade förordning om elektronisk identifiering (SOU 2024:45)

Remissinstanser

1. Alvesta kommun
2. Arbetsförmedlingen
3. Bolagsverket
4. Brottsförebyggande rådet
5. Brottsoffermyndigheten
6. Båstads kommun
7. Centrala studiestödsnämnden
8. CGI Sverige AB
9. Chalmers tekniska högskola AB
10. Comfact AB
11. Cybercom Group AB
12. Domstolsverket
13. E-hälsomyndigheten
14. Ekerö kommun
15. Ekobrottsmyndigheten
16. Ekonomistyrningsverket
17. Eskilstuna kommun
18. Finansiell ID-Teknik BID AB
19. Finansinspektionen

20. Fintech Sverige
21. Freja eID Group AB
22. Friskolornas riksförbund
23. Funktionsrätt Sverige
24. Färgelanda kommun
25. Företagarna
26. Försvarets materielverk
27. Försvarets radioanstalt
28. Försvarsmakten
29. Försäkringskassan
30. Förvaltningsrätten i Härnösand
31. Förvaltningsrätten i Stockholm
32. Göteborgs kommun
33. Heby kommun
34. Hofors kommun
35. Idéburna skolors riksförbund
36. Ideella Föreningen Teknikföretagen i Sverige
37. IIS – Internetstiftelsen i Sverige
38. Inera AB
39. Inspektionen för arbetslöshetsförsäkringen
40. Integritetsskyddsmyndigheten
41. Kalmar kommun
42. Kammarkollegiet
43. Kammarrätten i Stockholm
44. Knowit AB
45. Kommerskollegium
46. Konkurrensverket
47. Kriminalvården
48. Kungl. Tekniska högskolan
49. Kungsbacka kommun

50. Landsorganisationen i Sverige
51. Lantmäteriet
52. Linköpings kommun
53. Luleå kommun
54. Lunds kommun
55. Lunds Tingsrätt
56. Länsstyrelsen i Blekinge län
57. Länsstyrelsen i Gävleborgs län
58. Länsstyrelsen Norrbottens län
59. Länsstyrelsen i Skåne län
60. Länsstyrelsen i Stockholms län
61. Länsstyrelsen i Uppsala län
62. Länsstyrelsen i Västra Götalands län
63. Malmö kommun
64. Myndigheten för delaktighet
65. Myndigheten för digital förvaltning
66. Myndigheten för samhällsskydd och beredskap
67. Mölndals kommun
68. Nybro kommun
69. Pensionsmyndigheten
70. Polismyndigheten
71. Post- och telestyrelsen
72. Regelrådet
73. Region Dalarna
74. Region Norbotten
75. Riksarkivet
76. Riksbanken
77. Riksdagens ombudsmän
78. Robertsfors kommun
79. Scrive AB

80. Signicat AB
81. Skatteverket
82. Skövde kommun
83. Socialstyrelsen
84. Statens servicecenter
85. Statens skolverk
86. Statistiska centralbyrån
87. Statskontoret
88. Stockholms kommun
89. Storumans kommun
90. Strömstads kommun
91. Svensk e-identitet
92. Svenska bankföreningen
93. Svenskt Näringsliv
94. Sveriges advokatsamfund
95. Sveriges akademikers centralorganisation
96. Sveriges a-kassor
97. Sveriges ambassad i Berlin
98. Sveriges ambassad i London
99. Sveriges Kommuner och Regioner
100. Swedac
101. Swedish FinTech Association
102. Säkerhets- och försvarsföretagen
103. Säkerhetspolisen
104. TechSweden
105. Teknikföretagen
106. Telia AB
107. Tillväxtverket
108. Torsby kommun
109. Trafikverket

110. Tranemo kommun
111. Transportstyrelsen
112. Tranås kommun
113. Umeå universitet
114. Verket för innovationssystem
115. Vetenskapsrådet
116. Värnamo kommun
117. Västra Götalandsregionen
118. Ydre kommun
119. ZealiD AB
120. Åklagarmyndigheten
121. Älvsbyns kommun
122. Örnköldsviks kommun
123. Östersunds kommun
124. Överkalix kommun

Remissvaren ska ha kommit in till Finansdepartementet **senast den 1 november 2024**. Svaren bör lämnas per e-post till fi.remissvar@regeringskansliet.se och med kopia till fi.ofa.dof.remissor@regeringskansliet.se. Ange diarienummer Fi2024/01413 och remissinstansens namn i ämnesraden på e-postmeddelandet.

Svaret bör lämnas i två versioner: den ena i ett bearbetningsbart format (t.ex. Word), den andra i ett format (t.ex. pdf) som följer tillgänglighetskraven enligt lagen (2018:1937) om tillgänglighet till digital offentlig service. Remissinstansens namn ska anges i namnet på respektive dokument.

Remissvaren kommer att publiceras på regeringens webbplats.

I remissen ligger att regeringen vill ha synpunkter på förslagen eller materialet i betänkandet. Det är endast förslagen och materialet i själva betänkandet som remitteras och inte den externa rapport som kartlägger vissa kostnader som följer direkt av förordningen.

Myndigheter under regeringen är skyldiga att svara på remissen. En myndighet avgör dock på eget ansvar om den har några synpunkter att redovisa i ett svar. Om myndigheten inte har några synpunkter, räcker det att svaret ger besked om detta.

För **andra remissinstanser** innebär remissen en inbjudan att lämna synpunkter.

Betänkandet kan laddas ned från Regeringskansliets webbplats www.regeringen.se.

Remissinstanserna kan utan kostnad beställa tryckta exemplar av betänkandet via ett [beställningsformulär hos Elanders Sverige AB](#).

Råd om hur remissyttranden utformas finns i Statsrådsberedningens promemoria [Svara på remiss \(SB PM 2021:1\)](#). Den kan laddas ned från Regeringskansliets webbplats www.regeringen.se.

Johan Ndure
Departementsråd

Kopia till

Elanders Sverige AB, e-postadress: betankande@elanders.com

Kompletterande bestämmelser till EU:s reviderade förordning om elektronisk identifiering

*Slutbetänkande av Utredningen om
säker och tillgänglig digital identitet*

Stockholm 2024



STATENS OFFENTLIGA
UTREDNINGAR

SOU 2024:45

SOU och Ds finns på [regeringen.se](https://www.regeringen.se) under Rättsliga dokument.

Svara på remiss – hur och varför
Statsrådsberedningen, SB PM 2021:1.

Information för dem som ska svara på remiss finns tillgänglig på [regeringen.se/remisser](https://www.regeringen.se/remisser).

Layout: Kommittéservice, Regeringskansliet

Omslag: Elanders Sverige AB

Tryck och remisshantering: Elanders Sverige AB, Stockholm 2024

ISBN 978-91-525-0956-2 (tryck)

ISBN 978-91-525-0957-9 (pdf)

ISSN 0375-250X

Till statsrådet Erik Slottner

Regeringen beslutade den 22 december 2022 att tillkalla en särskild utredare med uppdrag att utreda och lämna förslag på hur staten kan utfärda en e-legitimation på högsta tillitsnivå. Utredaren skulle också se över behovet av anpassningar som följer av den reviderade eIDAS-förordningen.

Som särskild utredare förordnades från och med den 22 december 2022 rådmannen Henrik Arhede.

Som huvudsekreterare i utredningen anställdes från och med den 9 januari 2023 hovrättsassessorn Helena Forsaeus. Som utredningssekreterare anställdes från och med den 9 januari 2023 seniora handläggaren Björn Scharin och från och med den 23 januari 2023 hovrättsassessorn Anna Carlson.

Som sakkunniga förordnades från och med den 7 februari 2023 kanslirådet Richard Halltell (Finansdepartementet), ämnessakkunnige Magnus Thomann (Justitiedepartementet), departementssekreteraren Johanna Wasteson Lundberg (Finansdepartementet) och departementssekreteraren Ylva Wide (Finansdepartementet). Samma dag förordnades som experter strategen Anneli Hagdahl (Myndigheten för digital förvaltning), rättsliga experten Johannes Holmström (Skatteverket), digitaliseringsstrategen Torbjörn Karlsson (Sveriges Kommuner och Regioner), verksamhetsutvecklaren Ulf Palmgren (Försäkringskassan), strategiska projektledaren Fresia Perez (Sunet), stf. operativa chefen Mikaela Rosenlind Magnusson (Sveriges Certifieringsorgan för IT-säkerhet vid Försvarets materielverk), näringspolitiska experten Fredrik Sand (TechSverige), inspektören Björn Seeth (Polismyndigheten), seniora handläggaren Gustav Söderlind (Myndigheten för samhällsskydd och beredskap) och enhetschefen Helene Thorgren (Bolagsverket).

Johanna Wasteson Lundberg entledigades från sitt uppdrag som sakkunnig den 24 april 2023 och samma dag förordnades rättssak-

kunniga Malin Wictor (Finansdepartementet) att vara sakkunnig i utredningen. Helene Thorgren entledigades från sitt uppdrag som expert den 11 september 2023 och samma dag förordnades verksjuristen Lena Göransson Norrsjö (Bolagsverket) att vara expert i utredningen. Magnus Thomann entledigades från sitt uppdrag som sakkunnig den 20 november 2023 och samma dag förordnades ämnesrådet Eva Stengård (Kulturdepartementet) att vara sakkunnig i utredningen. Ulf Palmgren entledigades från sitt uppdrag som expert den 20 november 2023 och samma dag förordnades verksamhetsutvecklaren Azize Cuydur (Försäkringskassan) att vara expert i utredningen. Björn Seeth entledigades från sitt uppdrag som expert den 30 april 2024 och samma dag förordnades handläggaren Jacob Österlindh (Polismyndigheten) att vara expert i utredningen.

Utredningen redogör för uppdraget med användande av vi-form även om det inte funnits fullständig samsyn i alla delar. Utredningen, som har tagit sig namnet Utredningen om säker och tillgänglig identitet, överlämnade delbetänkandet *En säker och tillgänglig statlig e-legitimation* (SOU 2023:61) den 16 oktober 2023.

Utredningen överlämnar härmed slutbetänkandet *Kompletterande bestämmelser till EU:s reviderade förordning om elektronisk identifiering* (SOU 2024:45). Uppdraget är med detta slutfört.

Gränna i juni 2024

Henrik Ardhede

/Helena Forsaeus
Anna Carlson
Björn Scharin

Innehåll

Förkortningar	13
Sammanfattning	17
1 Författningsförslag	29
1.1 Förslag till lag om ändring i lagen (2016:561) om kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.....	29
1.2 Förslag till förordning om ändring i förordningen (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.....	42
1.3 Förslag till förordning om ändring i förordningen (2007:854) med instruktion för Försvarets materielverk.....	48
1.4 Förslag till förordning om ändring i förordningen (2007:951) med instruktion för Post- och telestyrelsen.....	49
1.5 Förslag till förordning om ändring i förordningen (2007:1110) med instruktion för Bolagsverket.....	52
1.6 Förslag till förordning om ändring i offentlighets- och sekretessförordningen (2009:641).....	53
1.7 Förslag till förordning om ändring i förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning.....	55

2	Utredningens uppdrag och arbete	57
2.1	Utredningens uppdrag	57
2.2	Utredningens arbete.....	58
2.3	Utredningens prioriteringar.....	58
2.4	Betänkandets disposition	58
3	Begrepp och termer	61
3.1	Identitetsbeteckningar	61
3.2	Identifiering och autentisering	63
3.3	E-legitimation	64
3.4	Den europeiska digitala identitetsplånboken.....	65
3.5	Förlitande part	65
3.6	Betrodda tjänster och de funktioner som utgör betrodda tjänster.....	66
3.6.1	Vad är betrodda tjänster?.....	66
3.6.2	De funktioner som utgör betrodda tjänster.....	66
4	EU:s förordning om elektronisk identifiering	71
4.1	Ramverk för gränsöverskridande elektronisk identifiering och betrodda tjänster	71
4.2	Översyn av förordningen	72
4.3	Skillnader i stora drag mellan den ursprungliga och den reviderade eIDAS-förordningen	75
4.4	Den reviderade förordningens struktur och innehåll.....	76
4.5	Allmänna bestämmelser	77
4.5.1	Syften	77
4.5.2	Tillämpningsområde	78
4.5.3	Definitioner	79
4.5.4	Inre marknadsprincipen.....	80
4.5.5	Användning av pseudonymer vid elektroniska transaktioner	80

4.6	Elektronisk identifiering.....	81
4.6.1	Ömsesidigt erkännande.....	81
4.6.2	Anmälningförfarande och tillitsnivåer.....	81
4.6.3	Säkerhetsincidenter och skadeståndsansvar.....	82
4.6.4	Gränsöverskridande identitetsmatchning.....	83
4.6.5	Interoperabilitet.....	84
4.6.6	Certifiering av e-legitimationssystem.....	85
4.6.7	Åtkomst till hård- och mjukvarufunktioner.....	85
4.7	Europeisk digital identitetsplånbok.....	86
4.7.1	Summarisk introduktion.....	86
4.7.2	En verktygslåda med en teknisk arkitektur- och referensram arbetas fram.....	90
4.7.3	Fyra pilotprojekt för att testa den digitala europeiska identitetsplånboken.....	91
4.7.4	Aktörer som är involverade i den europeiska digitala identitetsplånboken.....	92
4.7.5	Identitetsplånbokslösningen, identitetsplånboksinstansen och PID.....	97
4.8	Befintliga betrodda tjänster.....	101
4.8.1	Elektroniska underskrifter.....	101
4.8.2	Elektroniska stämplarna.....	105
4.8.3	Elektronisk tidsstämpling.....	107
4.8.4	Certifikat för autentisering av webbplatser.....	108
4.8.5	Elektronisk tjänst för rekommenderad leverans.....	108
4.9	Nya betrodda tjänster.....	110
4.9.1	Kvalificerade tjänster för förvaltning av anordningar för skapande av elektroniska underskrifter på distans.....	110
4.9.2	Elektroniska attributsintyg.....	110
4.9.3	Elektroniska arkiveringstjänster.....	114
4.9.4	Elektroniska liggare.....	115
4.10	Tillhandahållare av betrodda tjänster.....	116
4.10.1	Kvalificerade och icke-kvalificerade tillhandahållare.....	116
4.10.2	Säkerhetskrav och krav på incidentrapportering.....	116

4.10.3	Skillnader i skadeståndsansvar och bevisbörda ...	119
4.10.4	Krav på kvalificerade tillhandahållare.....	119
4.10.5	Tillsyn	120
4.10.6	Sanktioner.....	121
4.10.7	Förteckning över tillhandahållare och betrodda tjänster	122
4.11	Rättslig verkan av betrodda tjänster	122
4.11.1	Erkännande av betrodda tjänster från andra länder.....	123
5	Nationell reglering av elektronisk identifiering och betrodda tjänster	125
5.1	Svenska kompletterande bestämmelser.....	125
5.2	Tillsyn.....	126
6	Överväganden och förslag	129
6.1	Behovet av ytterligare kompletterande bestämmelser till den reviderade eIDAS-förordningen.....	129
6.2	Nya och ändrade nationella bestämmelser med anledning av den reviderade eIDAS-förordningen.....	131
6.3	Den europeiska digitala identitetsplånboken.....	133
6.3.1	Tillhandahållare av den europeiska digitala identitetsplånboken.....	133
6.3.2	Den tillhandahållande myndigheten får meddela vissa ytterligare föreskrifter	145
6.3.3	Tillhandahållare av uppgifter för personidentifiering.....	146
6.3.4	Elektroniska attributsintyg.....	156
6.3.5	Kostnadsfria valideringsmekanismer	160
6.3.6	Tillhandahållande av förteckningar för validering	162
6.3.7	Certifiering av den digitala europeiska identitetsplånboken och system för elektronisk identifiering	165
6.3.8	Tillhandahållandet förutsätter att åtgärder för ökad illgänglighet vidtas	170

6.3.9	Behandling av personuppgifter	172
6.3.10	Sekretess	185
6.4	Gränsöverskridande identitetsmatchning	187
6.5	Betrodda tjänster	196
6.5.1	Allmänt om bedömning av överensstämmelse	196
6.5.2	Krav på certifiering av betrodda tjänster	198
6.5.3	Krav på certifiering av anordningar	199
6.6	Ett styrningsramverk för tillsyn och samarbete	201
6.6.1	Tillsyn över den europeiska digitala identitetsplån boken	202
6.6.2	Tillsynsmyndigheten ska ansvara för registret över förlitande parter	208
6.6.3	Tillsynsmyndigheten ska agera vid säkerhetsincidenter	211
6.6.4	Tillsynsmyndigheten ska ha vissa ytterligare uppgifter	213
6.6.5	Tillsyn över betrodda tjänster	214
6.6.6	Tillsynsstrukturen för nationellt utfärdade e-legitimationer behöver ses över	215
6.6.7	Bestämmelser om administrativa sanktionsavgifter ska införas i kompletteringslagen	217
6.6.8	Överträdelser som ska leda till sanktionsavgift ...	220
6.6.9	Förfarandet vid beslut om sanktionsavgift	224
6.6.10	Sanktionsavgift ska bygga på strikt ansvar men inte vara obligatorisk	225
6.6.11	Sanktionsavgiftens storlek	228
6.6.12	Hinder mot sanktionsavgift	231
6.7	Överklagande	232
6.8	Identitetsplån bokens användningsområden för nationell effektivitet och nytta	233
6.9	Missbruk eller annan otillåten användning av identitetsplån boken	236
7	I kraftträdande- och övergångsbestämmelser	243

8	Konsekvenser	247
8.1	Inledning	247
8.2	Konsekvenser av den reviderade eIDAS-förordningen	247
8.3	Nollalternativ	250
8.4	Vilka myndigheter berörs av förslagen?	250
8.5	Förslaget om ansvar för tillhandahållande av en identitetsplånbok	250
8.5.1	Övriga tillkommande kostnader för att tillhandahålla identitetsplånboken	252
8.5.2	Förslaget om att tillhandahålla personidentifieringsuppgifter för fysiska personer	255
8.5.3	Förslaget om att tillhandahålla personidentifieringsuppgifter för juridiska personer	256
8.6	Förslaget om tillsyn över identitetsplånboken och förändrad tillsyn över betrodda tjänster	257
8.7	Förslaget om att tillhandahålla registret över förlitande parter	258
8.8	Konsekvenser för offentlig sektor i övrigt	259
8.8.1	Konsekvenser för domstolarna	259
8.8.2	Kommuner och regioner	259
8.9	Konsekvenser för företag	260
8.9.1	Berörda företag	260
8.9.2	Påverkan på företag inom området elektronisk identifiering	261
8.9.3	Påverkan på företag som tillhandahåller betrodda tjänster	264
8.9.4	Påverkan på övriga företag	264
8.10	Övriga konsekvenser	264
8.11	Tidpunkten för ikraftträdande och behovet av speciella informationsinsatser	265

9	Författningskommentar	267
9.1	Förslaget till lag om ändring i lagen (2016:561) om kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.....	267
9.2	Förslaget till förordning om ändring i förordningen (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.....	283
9.3	Förslaget till förordning om ändring i förordningen (2007:951) med instruktion för Post- och telestyrelsen	286
9.4	Förslaget till förordning om ändring i förordningen (2007:1110) med instruktion för Bolagsverket.....	288
9.5	Förslaget till ändring i offentlighets- och sekretessförordningen (2009:641)	288
9.6	Förslaget till förordning om ändring i förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning.....	289

Bilagor

Bilaga 1	Kommittédirektiv 2022:142	291
Bilaga 2	EU:s reviderade förordning om elektronisk identifiering.....	299
Bilaga 3	Författningar med hänvisning till EU:s förordning om elektronisk identifiering.....	355
Bilaga 4	Rapport av Governo AB, kostnadsuppskattning av eIDAS-förordningens bilaga VI.....	359

Förkortningar

EU-rättsakter m.m.

Den reviderade eIDAS-förordningen

Europaparlamentets och rådets förordning (EU) 2024/1183 av den 11 april 2024 om ändring av förordning (EU) nr 910/2014 vad gäller inrättandet av ett europeiskt ramverk för digital identitet

Förordningen om digitala marknader

Europaparlamentets och rådets förordning (EU) 2022/1925 av den 14 september 2022 om öppna och rättvisa marknader inom den digitala sektorn och om ändring av direktiv (EU) 2019/1937 och (EU) 2020/1828

Cybersäkerhetsakten

Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013,

EU:s förordning om en gemensam digital ingång

Europaparlamentets och rådets förordning (EU) 2018/1724 av den 2 oktober 2018 om inrättande av en gemensam digital ingång för tillhandahållande av information, förfaranden samt hjälp- och

	problemlösningstjänster och om ändring av förordning (EU) nr 1024/2012
EU:s dataskyddsförordning	Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG
eIDAS-förordningen	Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG
EU:s rättighetsstadga	Europeiska unionens stadga om de grundläggande rättigheterna
Europakonventionen	Den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna, med de tillägg och ändringar som gjorts genom de protokoll som Sverige ratificerat
EUCC	Kommissionens genomförandeförordning (EU) 2024/482 av den 31 januari 2024 om fastställande av tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) 2019/881 vad gäller antagande av den europeiska Common Criteria-baserade

	ordningen för cybersäkerhetscertifiering
NIS2-direktivet	Europaparlamentets och rådets direktiv av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148
<i>Övriga förkortningar</i>	
a.a.	anfört arbete
CSEC	Sveriges Certifieringsorgan för IT-säkerhet vid Försvarets materielverk
Digg	Myndigheten för digital förvaltning
Dir.	Kommittédirektiv
Ds	Departementsserien
ECATS	European Competent Authorities for Trust Services
EDICG	Den europeiska samarbetsgruppen för digital identitet (The European Digital Identity Cooperation Group)
Enisa	Europeiska unionens cybersäkerhetsbyrå
ETSI	European Telecommunications Standards Institute
EU	Europeiska unionen
f./ff.	följande sida/sidor

FESA	Forum of European Supervisory Authorities for trust service providers
FMV	Försvarets materielverk
ibid.	ibidem, eller på samma ställe, dvs. på samma sida/sidor som föregående fotnotsreferens
LPID	”Legal PID”, personidentifieringsuppgifter för juridiska personer
MSB	Myndigheten för samhällsskydd och beredskap
PID	”Personal identification data”, personidentifieringsuppgifter
Prop.	Regeringens proposition
PTS	Post- och telestyrelsen
SIS	Svenska institutet för standarder
SKR	Sveriges Kommuner och Regioner
SOU	Statens Offentliga Utredningar
SPAR	Statens personadressregister
Swedac	Styrelsen för ackreditering och teknisk kontroll

Sammanfattning

Uppdraget i korthet

Europaparlamentets och rådets förordning (EU) 2024/1183 av den 11 april 2024 om ändring av förordning (EU) nr 910/2014 vad gäller inrättandet av ett europeiskt ramverk för digital identitet (härefter benämnd den reviderade eIDAS-förordningen) innebär att en rad nya krav behöver mötas av medlemsstaterna och de aktörer som omfattas av förordningens tillämpningsområde. En betydande förändring är skyldigheten för medlemsstaterna att säkerställa att alla fysiska och juridiska personer i EU kan tillhandahållas en europeisk digital identitetsplånbok.

Med anledning av den reviderade förordningen har utredningen uttryckligen uppdragits att bl.a.

- *utreda* hur det kan säkerställas att en kostnadseffektiv digital identitetsplånbok ska utfärdas i enlighet med föreskrivna krav, och hur en sådan identitetsplånbok kan användas ändamålsenligt för största möjliga nationella effektivitet och nytta,
- *analysera* den slutgiltiga versionen av förordningen i sin helhet och ge förslag på hur Sverige kan uppfylla tillkommande krav, och
- *föreslå* nya eller ändrade författningsbestämmelser som är nödvändiga eller annars bedöms lämpliga för att komplettera den reviderade eIDAS-förordningen.

Att en politisk överenskommelse mellan Europaparlamentet och rådet träffades så sent som i november 2023 och att den reviderade eIDAS-förordningen trädde i kraft den 20 maj i år medför att utredningens överväganden och förslag, med hänsyn till uppdragets givna tidsram, omfattar enbart de anpassningar av svensk rätt som är absolut nödvändiga för att Sverige ska uppfylla förordningens krav avseende tillhand-

hållande av en europeisk digital identitetsplånbok och nationella bestämmelser om sanktionsavgifter vid regelöverträdelser som begås av kvalificerade och icke-kvalificerade tillhandahållare av betrodda tjänster. Utredningens arbete och prioriteringar redovisas i kap. 2.

I detta sammanhang bör även tilläggas att den reviderade eIDAS-förordningen, som förvisso utmärks av en tämligen hög detaljnivå, kommer att konkretiseras ytterligare genom ett flertal direkt tillämpliga genomförandeakter. Det medför att det för närvarande är svårt eller närmast omöjligt att få en full överblick av förordningens tillämpning och dess konsekvenser. I anslutning till beskrivningen av de konsekvenser som utredningens förslag bedöms ge upphov till redovisas i korthet även kommissionens konsekvensanalys av sitt förslag till reviderad eIDAS-förordning (se kap. 8).

Kommittédirektiven finns i bilaga 1 till detta betänkande.

Inrättandet av en europeisk digital identitetsplånbok

Enligt den direkt tillämpliga reviderade eIDAS-förordningen ska, som framgått, medlemsstaterna säkerställa tillhandahållandet av en europeisk digital identitetsplånbok. Syftet är att alla fysiska och juridiska personer i EU på ett säkert, tillitsbaserat och sömlöst sätt ska ges tillgång till publika och privata tjänster inom unionen online och, när det är lämpligt, i offlineläge.

De europeiska digitala identitetsplånböckerna ska tillhandahållas inom 24 månader efter ikraftträdande av kommissionens genomförandeakter med bl.a. referensstandarder för identitetsplånboken och dess certifiering. Dessa genomförandeakter ska antas senast den 21 november 2024.

Användningen av en europeisk digital identitetsplånbok ska vara frivillig och, för fysiska personer, avgiftsfri. Avsaknad av en sådan identitetsplånbok ska inte påverka tillgången till service eller möjligheten att bedriva verksamhet. Identitetsplånboken ska göras tillgänglig för personer med funktionsnedsättning på lika villkor i enlighet med bestämmelserna i Europaparlamentets och rådets direktiv (EU) 2019/882 av den 17 april 2019 om tillgänglighetskrav för produkter och tjänster.

Den europeiska digitala identitetsplånboken ska göra det möjligt för användaren att begära, erhålla, välja, kombinera, lagra, radera, dela

och visa upp uppgifter om personidentifiering. Med sådana personidentifieringsuppgifter, och i tillämpliga fall i kombination med elektroniska attributsintyg, ska användaren kunna autentisera sig gentemot bl.a. förlitande parter. Med förlitande part avses t.ex. en aktör som tillhandahåller en digital tjänst för vilken åtkomst ges efter att identifiering skett med exempelvis en europeisk digital identitetsplånbok eller en e-legitimation. Identitetsplånboken är i detta avseende ett medel för elektronisk identifiering.¹ Den ska således kunna användas för bl.a. det ändamålet.

Det är användaren som förser sin identitetsplånbok (benämns i betänkandet även plånboksinstans) med elektroniska attributsintyg. Med attribut avses egenskaper, kvaliteter, rättigheter eller tillstånd hos en fysisk eller juridisk person eller hos ett föremål.

All behandling av personuppgifter som utförs av tillhandahållare av den europeiska digitala identitetsplånboken som medel för elektronisk identifiering ska utföras i enlighet med lämpliga och effektiva dataskyddsåtgärder. Det ska kunna visas att behandlingen är förenlig med EU:s dataskyddsförordning.²

Den europeiska digitala identitetsplånboken beskrivs i avsnitt 4.7.

Tillhandahållare av den europeiska digitala identitetsplånboken

För att säkerställa att Sverige, inom föreskriven tid, uppfyller kraven som ställs på medlemsstaterna föreslås att regeringen utser en statlig myndighet med ansvar att tillhandahålla en europeisk digital identitetsplånbok till både fysiska och juridiska personer (*tillhandahållande myndighet*). En statligt tillhandahållen identitetsplånbok kan även öka robustheten i ekosystemet för elektronisk identifiering.

Myndigheten för digital förvaltning bedöms vara lämpad för uppgiften att tillhandahålla den europeiska digitala identitetsplånboken.

Vi föreslår samtidigt att Sverige tillvaratar möjligheten i den reviderade eIDAS-förordningen att författningsreglera att certifierade europeiska digitala identitetsplånböcker ska få tillhandahållas även av

¹ I eIDAS-förordningen, liksom i svensk kompletterande lagstiftning, används benämningen medel för elektronisk identifiering för det som i vardagligt tal kallas e-legitimation, se vidare avsnitt 3.3.

² Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

privata aktörer som godkänts för detta efter att ha genomgått ett anmälnings- och granskningsförfarande (*godkända tillhandahållare*). Det är ändamålsenligt att den tillhandahållande myndigheten ansvarar för denna granskning.

Villkor för ett sådant godkännande och utformningen för granskningsförfarandet får regleras på annan nivå än lag genom det föreskriftsbemyndigande som föreslås för regeringen eller den myndighet som regeringen bestämmer. Bemyndiganden att meddela föreskrifter föreslås även i fråga om dels ytterligare funktioner för de europeiska digitala identitetsplånböckerna, inbegripet interoperabilitet med befintliga nationella medel för elektronisk identifiering, dels undantag från förordningskravet att i vissa fall tillhandahålla öppen källkod.

För tillhandahållande av den europeiska digitala identitetsplånboken till juridiska personer får, enligt vårt förslag, en avgift tas ut av den tillhandahållande myndigheten.

Förslag och bedömningar finns i avsnitten 6.3.1 och 6.3.2.

Tillhandahållare av uppgifter för personidentifiering för den europeiska digitala identitetsplånboken

En förutsättning för användning av den europeiska digitala identitetsplånboken som medel för identifiering och för bl.a. lagring av elektroniska attributsintyg är att den förses med uppgifter för personidentifiering relaterade till en fysisk eller juridisk person. En i sammanhanget förekommande benämning är den engelska akronymen för ”personal identification data”, PID.

I den reviderade eIDAS-förordningen förutsätts att endast medlemsstaternas behöriga myndigheter kan fastställa identiteter med en hög tillförlitlighetsnivå och därmed garantera att en person faktiskt är den som personen påstår sig vara. Av den anledningen måste tillhandahållandet av de europeiska digitala identitetsplånböckerna bygga på den juridiska identiteten för unionsmedborgare, invånare i unionen och juridiska personer.

Därför föreslås att regeringen ska utse de statliga myndigheter som ska tillhandahålla elektroniska attesteringar av sådana uppgifter för personidentifiering för fysiska och juridiska personer som krävs för användningen av den europeiska digitala identitetsplånboken.

Även om det finns andra, i sig lämpade myndigheter, talar effektivitetsskäl för att den myndighet som av regeringen utses som tillhandahållare av den europeiska digitala identitetsplånboken också bör ansvara för att till identitetsplånboken tillhandahålla uppgifter för personidentifiering för fysiska personer.

När det gäller tillhandahållande av juridiska personers uppgifter för personidentifiering (med förkortningen LPID för "legal PID") finns det också tänkbara alternativ. Det finns inte en specifik myndighet i Sverige som har registreringsansvar för samtliga juridiska personer. Av effektivitetsskäl bör dock ett uppdelat ansvar undvikas. Det föreslås därför att regeringen utser en och samma myndighet att tillhandahålla uppgifter för personidentifiering för juridiska personer. Vi förordar att Bolagsverket ges denna uppgift.

För tillhandahållande av uppgifter för personidentifiering till juridiska personer får, enligt vårt förslag, en avgift tas ut av den myndighet som tillhandahåller sådana uppgifter.

Förslag och bedömningar redovisas i avsnitt 6.3.3.

Tillhandahållare av kostnadsfria valideringsmekanismer och förteckningar för validering

Medlemsstaterna ska enligt den reviderade eIDAS-förordningen tillhandahålla kostnadsfria valideringsmekanismer för de europeiska digitala identitetsplånböckerna. Sådana valideringsmekanismer syftar till att dels säkerställa att europeiska digitala identitetsplånböckers äkthet och giltighet kan kontrolleras, dels göra det möjligt för användare av europeiska digitala identitetsplånböcker att kontrollera äkthet och giltighet för identiteten hos registrerade förlitande parter.

För att säkerställa att kraven på att möjliggöra föreskriven validering uppfylls över tid, föreslås att regeringen utser två statliga myndigheter med uppgift att tillhandahålla kostnadsfria valideringsmekanismer i enlighet med den reviderade eIDAS-förordningen.

Det framstår, enligt vår bedömning, som ändamålsenligt att valideringsmekanismerna tillhandahålls av den myndighet som av regeringen utses att tillhandahålla den europeiska digitala identitetsplånboken respektive tillsynsmyndigheten som ansvarar för registret över förlitande parter (se nedan).

Beroende av vilka tekniska lösningar som används för validering kan det behöva upprättas, underhållas och offentliggöras sådana förteckningar som möjliggör valideringen. Detta gäller även validering av uppgifter för personidentifiering för den europeiska digitala identitetsplån-boken. Det är tillhandahållarna som ska tillse att validering är möjlig.

Förslag och bedömningar redovisas i avsnitt 6.3.5 och 6.3.6.

Certifiering av den europeiska digitala identitetsplån-boken och system för elektronisk identifiering

Att den europeiska digitala identitetsplån-boken uppfyller kraven i den reviderade eIDAS-förordningen ska certifieras av ett, av varje medlemsstat, utpekat organ för bedömning av överensstämmelse. Certifieringskravet framgår således direkt av förordningen, som också föreskriver bl.a. att certifieringen ska vara giltig i högst fem år och villkoras av att en sårbarhetsbedömning genomförs med intervall om två år.

Certifieringen av identitetsplån-boken, liksom system för elektronisk identifiering, avser i huvudsak överensstämmelse med föreskrivna cybersäkerhetskrav och ska bygga på de relevanta europeiska ordningar för cybersäkerhetscertifiering som inrättats i enlighet med Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten).

Regeringen eller den myndighet som regeringen bestämmer ska, enligt lämnat förslag, utse ansvarigt organ för certifiering av europeiska digitala identitetsplån-böcker och system för elektronisk identifiering. Det bedöms vara ändamålsenligt att certifieringen utförs av certifieringsorgan som är ackrediterade enligt cybersäkerhetsakten. För svenskt vidkommande är det således Försvarets materielverk som är bäst lämpat för uppgiften att utse ansvarigt organ för certifiering av dels europeiska digitala identitetsplån-böcker, dels system för elektronisk identifiering i Sverige.

För det begränsade utrymme för nationella certifieringsordningar som lämnas i den reviderade eIDAS-förordningen finns behov av ett

föreskriftsbemyndigande. Utrymmet för den nationella certifieringsordningen omfattar dels andra områden än cybersäkerhet, dels sådana cybersäkerhetskrav som inte täcks av någon cybersäkerhetscertifieringsordning enligt cybersäkerhetsakten. De senare kraven torde ha nära koppling till tillhandahållandet av den europeiska digitala identitetsplånboken samt granskning och godkännande av privata aktörer som tillhandahållare av sådana identitetsplånböcker. Med beaktande av tidigare redovisad bedömning avseende ansvaret för den statligt tillhandahållna europeiska digitala identitetsplånboken och förslaget om granskningsförfarande för godkännande som tillhandahållare av en sådan identitetsplånbok, är det lämpligt att Myndigheten för digital förvaltning, i förekommande fall, och med stöd av förslaget föreskriftsbemyndigande, tar fram en sådan nationell certifieringsordning.

Förslag och bedömningar finns i avsnitt 6.3.7.

Register över förlitande parter

En förlitande part som avser att förlita sig på europeiska digitala identitetsplånböcker för tillhandahållande av offentliga eller privata tjänster genom digital interaktion ska enligt den reviderade eIDAS-förordningen registrera sig i den medlemsstat där den är etablerad.

Registreringen är avsedd att underlätta medlemsstaternas kontroller av lagenligheten hos de förlitande parternas verksamhet i enlighet med unionsrätten och syftar till att öka öppenheten i och förtroendet för användningen av sådana identitetsplånböcker. Av registrerade uppgifter ska bl.a. framgå vilka uppgifter som den förlitande parten, vid tillhandahållande av sina tjänster, avser att begära från användare; några andra än dessa uppgifter får inte begäras utan en föregående omregistrering.

Med hänsyn till hur regleringen om registret för förlitande parter är utformad i den reviderade eIDAS-förordningen föreslås att ansvaret för detta register ska åvila tillsynsmyndigheten över ramverket över den europeiska digitala identitetsplånboken, se vidare nedan.

Förslaget redovisas i avsnitt 6.6.2.

Tillsyn över den europeiska digitala identitetsplån-boken

Av den reviderade eIDAS-förordningen framgår att varje medlemsstat ska utse ett eller flera tillsynsorgan inom dess territorium som ska ansvara för tillsyn över ramverket för den europeiska digitala identitetsplån-boken och ges erforderliga befogenheter och tillräckliga resurser för att kunna utföra sin uppgift på ett ändamålsenligt, effektivt och oberoende sätt.

Vi föreslår därför att den myndighet som regeringen bestämmer ska ges ansvar att utöva tillsyn över att tillhandahållare av europeiska digitala identitetsplån-böcker som är etablerade i Sverige efterlever dels kraven i den reviderade eIDAS-förordningen och de rättsakter som meddelas med stöd av densamma, dels kraven i lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering (kompletteringslagen) och de föreskrifter som meddelas med stöd av densamma.

Med beaktande av den reviderade eIDAS-förordningens föreskrivna tillsynsbefogenheter bör bestämmelsen om tillsyn över den europeiska digitala identitetsplån-boken och dess tillhandahållare, med undantag för möjligheten att förena förelägganden och förbud med vite, motsvara vad som enligt gällande bestämmelser i kompletteringslagen föreskrivs i fråga om tillhandahållare av betrodda tjänster.

Om europeiska digitala identitetsplån-böcker, föreskrivna valideringsmekanismer, eller det system för elektronisk identifiering inom ramen för vilket sådana identitetsplån-böcker tillhandahålls är föremål för incidenter eller delvis äventyras på ett sätt som påverkar deras tillförlitlighet, eller tillförlitligheten för andra europeiska digitala identitetsplån-böcker, ska den medlemsstat som tillhandahöll dessa identitetsplån-böcker utan onödigt dröjsmål vidta åtgärder i enlighet med den reviderade eIDAS-förordningen. Det handlar om att tillfälligt upphäva tillhandahållandet och användningen av europeiska digitala identitetsplån-böcker, eller att återkalla dessa, om det är motiverat mot bakgrund av allvaret i ifrågavarande säkerhetsincident eller händelsen som äventyrat tillförlitligheten. För att säkerställa att dessa åtgärder vidtas på föreskrivet sätt ska detta ingå i ansvaret för den av regeringen utsedda tillsynsmyndigheten.

Det föreslås vidare att regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten ska få meddela föreskrifter om skyldig-

het för tillhandahållare av en europeisk digital identitetsplånbok att betala avgift för tillsynsmyndighetens verksamhet.

Ett samlat tillsynsansvar över både tillhandahållare av betrodda tjänster och tillhandahållare av den europeiska digitala identitetsplånboken bedöms medföra samordningsvinster som i sin tur kan förväntas leda till ökad kostnadseffektivitet när det gäller tillsyn på digitaliseringsområdet. Post- och telestyrelsen bör därför utses som tillsynsorgan över ramverket för den europeiska digitala identitetsplånboken.

Av den reviderade eIDAS-förordningen följer att tillsynsorgan får söka ömsesidigt bistånd från varandra för att underlätta tillsynen och efterlevnaden av skyldigheterna enligt förordningen. De berörda medlemsstaterna ska i enlighet med sin nationella rätt besluta om och inrätta arrangemang och förfaranden för gemensamma åtgärder som ska vidtas inom ramen för det ömsesidiga biståndet. För att säkerställa att detta krav uppfylls föreslås att Post- och telestyrelsen, i egenkap av tillsynsmyndighet, bemyndigas att meddela föreskrifter i nämnda avseenden.

Post- och telestyrelsen föreslås också utgöra den gemensamma kontaktpunkten för betrodda tjänster, europeiska digitala identitetsplånböcker och anmälda system för elektronisk identifiering i enlighet med det som föreskrivs i den reviderade eIDAS-förordningen.

Förslag och bedömningar finns i avsnitten 6.6.1, 6.6.3 och 6.6.4.

Administrativa sanktionsavgifter

Av den reviderade eIDAS-förordningen följer, i likhet med tidigare, att medlemsstaterna ska fastställa bestämmelser om effektiva, proportionerliga och avskräckande sanktioner. Därutöver föreskrivs att medlemsstaterna ska säkerställa att överträdelser av förordningen, som begås av kvalificerade och icke-kvalificerade tillhandahållare av betrodda tjänster, ska medföra administrativa sanktionsavgifter som ska uppgå till vissa lägsta maximinivåer.

Vi bedömer att omständigheterna motiverar att en tillsynsmyndighet och inte domstol beslutar om sanktionsavgifter. Det föreslås därför att tillsynsmyndigheten ska besluta om sådana sanktionsavgifter. Bestämmelser om detta tas in i kompletteringslagen, liksom bestämmelser om sanktionsavgifternas beloppsnivåer och omständigheter som ska beaktas när sådana avgifter bestäms. Tillsynsmyndighetens

beslut om sanktionsavgift ska få överklagas till allmän förvaltningsdomstol.

För att upprätthålla kravet på förutsägbarhet ska endast sådana överträdelse som tydligt kan avgränsas, och som inte kräver ett alltför stort mått av tolkning, kunna föranleda beslut om sanktionsavgift. I kompletteringslagen ska därför preciseras vilka överträdelse det är fråga om. Regleringen ska bygga på strikt ansvar. Det ska inte vara obligatoriskt att ta ut sanktionsavgift för de i lagen uppräknade överträdelse. Av lagen ska också framgå att sanktionsavgifter inte får beslutas om överträdelse omfattas av ett föreläggande om vite och överträdelse ligger till grund för en ansökan om utdömande av vitet. I lagen ska även införas bestämmelse om förfarandet vid beslut om sanktionsavgifter, såsom delgivningskrav, verkställighet och preskription.

Förslagen redovisas i avsnitten 6.6.7–6.6.12.

Författningsreglering

Den lagreglering som är nödvändig med anledning av inrättandet av en europeisk digital identitetsplånbok och kraven om utfärdande av sanktionsavgifter ska, enligt förslagen, införas huvudsakligen i lagen med kompletterande bestämmelse till EU:s förordning om elektronisk identifiering. I lagen tas även in centrala bestämmelse om behandling av personuppgifter som föranleds av tillhandahållandet av den europeiska digitala identitetsplånboken.

För att omfatta även de tillkommande beslut som enligt lämnade förslag får fattas enligt dels den reviderade eIDAS-förordningen med kommande tillhörande genomförandeakter, dels kompletteringslagen och föreskrifter som meddelas med stöd av densamma, ändras gällande bestämmelse om överklagande på så sätt att det framgår att den inte endast gäller beslut som meddelats av tillsynsmyndigheten.

Vissa övriga bestämmelse, bl.a. sådana som behövs för verkställigheten av kompletteringslagen, införas i förordningen (2016:576) med kompletterande bestämmelse till EU:s förordning om elektronisk identifiering.

Våra förslag medför behov av följdändringar i bl.a. offentlighets och sekretessförordningen (2009:641). Tillägg behöver också göras i respektive myndighetsinstruktion för de myndigheter som av reger-

ingen utses för nytt eller utökat ansvar i egenskap av dels tillhandahållare av den europeiska digitala identitetsplånboken, dels tillhandahållare av sådana elektroniska attesteringar av uppgifter för personidentifiering som ska kunna kopplas till en sådan identitetsplånbok (PID och LPID), dels ansvarigt organ att utöva tillsyn över ramverket för den europeiska digitala identitetsplånboken enligt den reviderade EU-förordningen.

Ny och ändrad reglering föreslås träda i kraft den 1 oktober 2025.

Förslag och bedömningar redovisas i avsnitten 6.2, 6.3.9, 6.3.10 och 6.7 samt i kapitel 7.

1 Författningsförslag

1.1 Förslag till lag om ändring i lagen (2016:561) om kompletterande bestämmelser till EU:s förordning om elektronisk identifiering

Härigenom föreskrivs i fråga om lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering¹

dels att 3 § ska upphöra att gälla,

dels att rubriken närmast före 3 § ska utgå,

dels att nuvarande 1 a–1 d ska betecknas 2–5 §§, 2 § ska betecknas 16 §, 4–6 §§ ska betecknas 17–19 §§, 7 § ska betecknas 29 § och 8 § ska betecknas 31 §,

dels att 1 § och nya 16, 17, 19, 29 och 31 §§ ska ha följande lydelse,

dels att rubrikerna närmast före 2, 4, 7 och 8 §§ ska sättas närmast före 16, 17, 29 och 31 §§,

dels att det ska införas tjugo nya paragrafer, 6–15 §§, 20–28 §§ och 30 § av följande lydelse,

dels att det närmast före 6, 10, 11, 15 och 20 §§ ska införas rubriker av följande lydelse.

¹ Senaste lydelse av

1 a § 2021:320

1 b § 2021:320

1 c § 2021:320

1 d § 2021:320.

Nuvarande lydelse

Föreslagen lydelse

Inledande bestämmelser

1 §²

Denna lag kompletterar Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, *i den ursprungliga lydelsen* (EU:s förordning om elektronisk identifiering).

Denna lag kompletterar Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (EU:s förordning om elektronisk identifiering).

Termer och uttryck i lagen har samma betydelse som i EU:s förordning om elektronisk identifiering.

Såvitt gäller behandling av personuppgifter kompletterar denna lag Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), här benämnd EU:s dataskyddsförordning.

Vid sådan behandling av personuppgifter som omfattas av EU:s dataskyddsförordning gäller även lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning och föreskrifter som har meddelats i anslutning till den lagen, om inte annat

² Senaste lydelse 2016:562.

följer av denna lag eller föreskrifter som meddelats i anslutning till lagen.

Europeisk digital identitetsplånbok

6 §

Regeringen bestämmer vilken myndighet som ska tillhandahålla den europeiska digitala identitetsplånboken i enlighet med artikel 5a.2 i EU:s förordning om elektronisk identifiering (tillhandahållande myndighet).

Den europeiska digitala identitetsplånboken får tillhandahållas även av den som, efter granskning, har godkänts av den tillhandahållande myndigheten (godkänd tillhandahållare).

7 §

För ett godkännande som avses i 6 § andra stycket krävs att villkoren för den europeiska digitala identitetsplånboken, liksom för att tillhandahålla en sådan, är uppfyllda i enlighet med EU:s förordning om elektronisk identifiering och de rättsakter som meddelats med stöd av förordningen samt denna lag och föreskrifter som meddelats med stöd av lagen.

Om det, efter ett godkännande, finns anledning att anta att villkoren enligt första stycket inte är uppfyllda ska den tillhandahållande myndigheten snarast underrätta

den myndighet som avses i 17 § om detta.

Regeringen eller den myndighet regeringen bestämmer ska meddela föreskrifter om villkor för godkännande och om anmälnings- och granskningsförfarandet enligt 6 § andra stycket.

8 §

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om:

1. sådana undantag från kravet att tillhandahålla öppen källkod som avses i artikel 5a.3 i EU:s förordning om elektronisk identifiering, och

2. sådana ytterligare funktioner för den europeiska digitala identitetsplånboken som avses i artikel 5a.7 i EU:s förordning om elektronisk identifiering.

9 §

Regeringen bestämmer vilken eller vilka myndigheter som ska tillhandahålla sådana uppgifter för personidentifiering som avses i artikel 3 i EU:s förordning om elektronisk identifiering, och som ska kunna kopplas till den europeiska digitala identitetsplånboken.

Kostnadsfria valideringsmekanismer

10 §

Den statliga myndighet som regeringen bestämmer ska tillhandahålla

1. en kostnadsfri valideringsmekanism som säkerställer att europeiska digitala identitetsplånböckers äkthet och giltighet kan kontrolleras.

2. En kostnadsfri valideringsmekanism som gör det möjligt för användare av europeiska digitala identitetsplånböcker att kontrollera äkthet och giltighet för identiteten hos de förlitande parter som registrerats enligt 17 § 3.

Behandling av personuppgifter för tillhandahållande och återkallelse av den europeiska digitala identitetsplånboken

11 §

Den tillhandahållande myndigheten ska med hjälp av automatiserad behandling föra en databas med en samling uppgifter om de europeiska digitala identitetsplånböcker som myndigheten har tillhandahållit.

Regeringen eller den myndighet som regeringen bestämmer får med stöd av 8 kap. 7 § regeringsformen meddela ytterligare föreskrifter om vilka uppgifter databasen ska innehålla och den längsta tid

som personuppgifter får behandlas i databasen.

12 §

Den tillhandahållande myndigheten får behandla personuppgifter om det är nödvändigt för att handlägga ärenden om tillhandahållande och återkallelse av giltigheten av en europeisk digital identitetsplånbok samt nödvändig administration av databasen över europeiska digitala identitetsplånböcker.

Personuppgifter som avses i första stycket får också behandlas om det är nödvändigt för att fullgöra uppgiftsutlämnande som sker i överensstämmelse med lag eller förordning.

13 §

Uppgifter om lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden får inte användas som sökbegrepp i databasen över europeiska digitala identitetsplånböcker.

Regeringen eller den myndighet som regeringen bestämmer får med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om integritetshöjande åtgärder till skydd för personuppgifter i verksamheten med tillhandahållandet av den europeiska digitala identitetsplånboken.

14 §

Artikel 21.1 i EU:s dataskyddsförordning om rätten att göra invändningar gäller inte vid sådan behandling av personuppgifter som är tillåten enligt denna lag eller föreskrifter som meddelats i anslutning till lagen.

Certifiering

15 §

Regeringen eller den myndighet som regeringen bestämmer ska utse ansvarigt organ för certifiering av europeiska digitala identitetsplånböcker, system för elektronisk identifiering, anordningar för skapande av kvalificerade elektroniska underskrifter och anordningar för skapande av kvalificerade elektroniska stämplor.

Granskning av kvalificerade tillhandahållare av betrodda tjänster16 §³

Bestämmelser om ackreditering av sådana organ för bedömning av överensstämmelse som i enlighet med artikel 20 i EU:s förordning om elektronisk identifiering ska granska kvalificerade tillhandahållare av betrodda tjänster, finns i Europaparlamentets och rådets förordning (EG) nr 765/2008 om krav för ackreditering och upphävande av förordning (EEG) nr 339/93 och i lagen (2011:791) om ackreditering och teknisk kontroll.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om krav för ackreditering av organ för bedöm-

³ Senaste lydelse 2022:1134.

ning av överensstämmelse, hur bedömningar av överensstämmelse ska göras, och rapportering av bedömningar av överensstämmelse.

Tillsyn

17 §

Den myndighet som regeringen bestämmer (tillsynsmyndigheten) ska

- | | |
|--|--|
| <p>1. fullgöra tillsynsorganets uppgifter enligt EU:s förordning om elektronisk identifiering och rättsakter som har meddelats med stöd av den förordningen, <i>och</i></p> <p>2. utöva tillsyn över efterlevnaden av denna lag och föreskrifter som har meddelats med stöd av lagen</p> | <p>1. fullgöra tillsynsorganets uppgifter enligt EU:s förordning om elektronisk identifiering och rättsakter som har meddelats med stöd av den förordningen,</p> |
|--|--|

3. upprätta, underhålla och offentliggöra en förteckning över förlitande parter och uppgifter om dessa i enlighet med artikel 5b.2 och 5b.5 i EU:s förordning om elektronisk identifiering, och

4. vidta nödvändiga åtgärder i enlighet med artikel 5e.1–3 i EU:s förordning om elektronisk identifiering vid säkerhetsincidenter som rör i artikeln angivna europeiska digitala identitetplånböcker, valideringsmekanismer eller det system för elektronisk identifiering inom ramen för vilket de europeiska digitala identitetplånböckerna tillhandahålls.

Tillsynsmyndigheten får meddela föreskrifter om sådana arrangemang och förfaranden för ömsesidigt bestånd som avses i artikel 46d i EU:s förordning om elektronisk identifiering.

19 §

Tillsynsmyndigheten får meddela de förelägganden och förbud som behövs för efterlevnaden av

1. EU:s förordning om elektronisk identifiering och rättsakter som har meddelats med stöd av den förordningen, och

2. denna lag och föreskrifter som har meddelats med stöd av lagen.

Förelägganden och förbud får förenas med vite. Förelägganden och förbud som riktas mot tillhandahållare av betrodda tjänster får förenas med vite.

Tillsynsmyndigheten får bestämma att beslut enligt första stycket ska gälla omedelbart.

*Administrativa
sanktionsavgifter för betrodda
tjänster*

20 §

Tillsynsmyndigheten får besluta om sanktionsavgifter enligt EU:s förordning om elektronisk identifiering i dess lydelse enligt Europaparlamentets och rådets förordning (EU) 2024/1183 av den 11 april 2024 om ändring av förordning (EU) nr 910/2014 vad gäller inrättandet av ett europeiskt ramverk för digital identitet. Sådana sanktionsavgifter får tas ut av kvalificerade och icke-kvalificerade tillhandahållare av betrodda tjänster som

1. utger sig för att vara en kvalificerad tillhandahållare utan att vara det eller tillhandahåller en icke-kvalificerad betrodd tjänst som utges vara kvalificerad,

2. har lämnat oriktiga eller ofullständiga uppgifter vid ansökan om att bli kvalificerad,

3. innehar status som kvalificerad tillhandahållare av betrodda tjänster eller har en kvalificerad betrodd tjänst, och inte i enlighet med artikel 24.2 a i nämnda förordning informerar om någon ändring av tillhandahållandet av tjänsten eller en avsikt att upphöra med verksamheten,

4. missbrukar EU-förtroendemärket för kvalificerade betrodda tjänster,

5. underlåter att rapportera om sådana incidenter som ska rapporteras enligt artikel 19a.1 b och artikel 24.2 fb i nämnda förordning, eller

6. överträder ett beslut av tillsynsmyndigheten om föreläggande som innebär ett förbud.

21 §

En sanktionsavgift ska för fysiska personer bestämmas till lägst 5 000 kronor och högst ett belopp motsvarande 5 miljoner euro.

En sanktionsavgift för juridiska personer ska bestämmas till lägst 5 000 kronor och högst det högsta av ett belopp motsvarande 5 miljoner euro respektive en procent av den totala globala årsomsättningen för det företag som tillhandahållaren av betrodda tjänster tillhörde under det räkenskapsår som föregick det år då överträdelsen inträffade.

22 §

När sanktionsavgiftens storlek bestäms ska särskild hänsyn tas till berörd enhets storlek, affärsmo­deller och överträdelse­r­nas allvar.

23 §

Tillsynsmyndigheten ska få sätta ner sanktionsavgiften helt eller delvis om överträdelsen är ringa eller ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften.

24 §

En sanktionsavgift får inte beslutas om överträdelsen omfattas av ett föreläggande om vite och överträdelsen ligger till grund för en ansökan om utdömande av vitet.

25 §

En sanktionsavgift får endast beslutas om den som avgiften ska tas ut av har fått tillfälle att yttra sig inom två år från det att överträdelsen ägde rum.

Ett beslut om sanktionsavgift ska delges.

26 §

Sanktionsavgiften tillfaller staten.

27 §

En sanktionsavgift ska betalas till tillsynsmyndigheten inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft

eller inom den längre tid som anges i beslutet.

Om sanktionsavgiften inte betalas inom föreskriven tid, ska myndigheten lämna den obetalda avgiften för indrivning.

Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m. Vid indrivning får verkställighet ske enligt utsökningsbalken.

28 §

En beslutad sanktionsavgift faller bort till den del beslutet om avgiften inte har verkställts inom fem år från det att beslutet fick laga kraft.

Avgifter

Regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten får meddela föreskrifter om skyldighet för tillhandahållare av betrodda tjänster att betala avgift för tillsynsmyndighetens verksamhet enligt denna lag.

29 §

Regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten får meddela föreskrifter om skyldighet för tillhandahållare av *europiska digitala identitetsplånböcker* att betala avgift för tillsynsmyndighetens verksamhet enligt denna lag.

30 §

Regeringen eller, efter regeringens bemyndigande, de myndigheter som avses i 6 § första stycket och 9 § får meddela föreskrifter om skyldighet för juridiska personer att betala avgift för att tillhandahållas en europeisk digital identitetsplånbok respektive uppgifter för personidentifiering enligt denna lag och föreskrifter som meddelats med stöd av den.

Överklagande

31 §

Tillsynsmyndighetens beslut enligt EU:s förordning om elektronisk identifiering och rättsakter som har meddelats med stöd av den förordningen, samt enligt denna lag och föreskrifter som har meddelats med stöd av lagen, får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Beslut av den myndighet som tillhandahåller uppgifter för personidentifiering liksom den tillhandahållande myndighetens och tillsynsmyndighetens beslut enligt EU:s förordning om elektronisk identifiering och rättsakter som har meddelats med stöd av den förordningen, samt enligt denna lag och föreskrifter som har meddelats med stöd av lagen får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

-
1. Denna lag träder i kraft den 1 oktober 2025.
 2. Äldre bestämmelser gäller för överträdelse som ägt rum före ikraftträdandet.

1.2 Förslag till förordning om ändring i förordningen (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering

Härigenom föreskrivs i fråga om förordningen (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering¹

dels att 2 och 3 §§ ska upphöra att gälla,

dels att nuvarande 4 och 5 §§ ska betecknas 15 och 16 §§, och 6–10 §§ ska betecknas 2–6 §§,

dels att nya 2 och 4 §§ och rubriken närmast för 2 § ska ha följande lydelse,

dels att rubriken närmast före nya 15 § ska lyda ”Tillsyn”,

dels att det ska införas åtta nya paragrafer, 7–14 §§, av följande lydelse,

dels att det närmast före 7 och 14 §§ ska införas rubriker av följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

Elektronisk identifiering

Anslutningsskyldigheten i 1 a § lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering gäller inte för Säkerhetspolisen eller myndigheter som hör till Försvarsdepartementet.

² §²
Anslutningsskyldigheten i 2 § lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering gäller inte för Säkerhetspolisen eller myndigheter som hör till Försvarsdepartementet.

¹ Senaste lydelse av

7 § 2021:321

9 § 2021:321

10 § 2021:321.

² Senaste lydelse 2021:321.

4 §³

Myndigheten för digital förvaltning ska till noden för inkommande gränsöverskridande elektronisk identifiering på begäran ansluta dem som uppfyller kraven för en sådan anslutning trots att de inte omfattas av anslutningsskyldigheten i 1 a § lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

Myndigheten får ta ut avgifter av de privata aktörer som har anslutit sig till noden för inkommande gränsöverskridande elektronisk identifiering som myndigheten tillhandahåller.

Myndigheten för digital förvaltning ska till noden för inkommande gränsöverskridande elektronisk identifiering på begäran ansluta dem som uppfyller kraven för en sådan anslutning trots att de inte omfattas av anslutningsskyldigheten i 2 § lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

Europeisk digital identitetsplånbok

7 §

Myndigheten för digital förvaltning ska vara den tillhandahållande myndigheten enligt 6 § första stycket lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering såvitt avser tillhandahållandet av en europeisk digital identitetsplånbok för både fysiska och juridiska personer.

8 §

Myndigheten för digital förvaltning ska meddela föreskrifter om villkor för godkännande som tillhandahållare av en europeisk digital identitetsplånbok och hur granskningsförfarandet enligt 6 § andra

³ Senaste lydelse 2021:321.

stycket lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering ska gå till,

Myndigheten får meddela föreskrifter om

1. sådana undantag från kravet att tillhandahålla öppen källkod som avses i artikel 5a.3 i EU:s förordning om elektronisk identifiering, och

2. sådana ytterligare funktioner för den europeiska digitala identitetsplånboken som avses i artikel 5a.7 i EU:s förordning om elektronisk identifiering.

9 §

Myndigheten för digital förvaltning ska i fråga om fysiska personer tillhandahålla sådana uppgifter för personidentifiering som avses i artikel 3 i EU:s förordning om elektronisk identifiering, och som ska kunna kopplas till den europeiska digitala identitetsplånboken.

Bolagsverket ska i fråga om juridiska personer tillhandahålla sådana uppgifter för personidentifiering som avses i artikel 3 i EU:s förordning om elektronisk identifiering, och som ska kunna kopplas till den europeiska digitala identitetsplånboken.

Myndigheterna får ta ut avgift av en juridisk person som tillhandahåller en europeisk digital identitetsplånbok och uppgifter för personidentifiering.

10 §

Myndigheten för digital förvaltning ska tillhandahålla en sådan valideringsmekanism som avses i 10 § 1 lagen (2016:561) om elektronisk identifiering.

Post- och telestyrelsen ska tillhandahålla en sådan valideringsmekanism som avses i 10 § 2 lagen om elektronisk identifiering.

11 §

Den databas som Myndigheten för digital förvaltning ska föra enligt 11 § lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering ska i fråga om en fysisk person innehålla

1. fullständigt namn, personnummer alternativt samordningsnummer för personer med styrkt identitet, och födelsetid för användaren av den tillhandahållna europeiska digitala identitetsplånboken,

2. uppgift om det medel för elektronisk identifiering med vilket användaren har styrkt sin identitet,

3. uppgift som på ett unikt sätt identifierar den tillhandahållna europeiska digitala identitetsplånboken, och

4. uppgift om status för en tillhandahållen europeisk digital identitetsplånbok, om den har återkallats samt skälen för det.

Utöver det som anges i första stycket 3–4 ska databasen, i fråga

om en juridisk person, innehålla uppgifter om dess namn och organisationsnummer.

12 §

Databasen som avses i 11 § får tillföras sådana uppgifter från Skatteverkets folkbokföringsdatabas som anges i 11 § första stycket 1.

13 §

Uppgifter och handlingar vilka finns i databasen som avses i 11 § ska gallras senast tio år efter utgången av det kalenderår då

- 1. den europeiska digitala identitetsplån boken tillhandahölls, eller*
- 2. ett ärende om återkallelse avslutades.*

Myndigheten för digital förvaltning får meddela närmare föreskrifter om integritetshöjande åtgärder till skydd för personuppgifter i databasen.

Certifiering

14 §

Försvarets materielverk ska utse ansvarigt organ för sådan certifiering av den europeiska digitala identitetsplån boken och system för elektronisk identifiering som avses i artikel 5c.1 i EU:s förordning om elektronisk identifiering samt ansvarigt organ för certifiering av sådana anordningar för skapande av kvalificerade elektroniska underskrifter och anord-

ningar för skapande av kvalificerade elektroniska stämplatser som avses i artikel 30 och 39 i nämnd förordning.

Denna förordning träder i kraft den 1 oktober 2025.

1.3 Förslag till förordning om ändring i förordningen (2007:854) med instruktion för Försvarets materielverk

Härigenom föreskrivs att 5 § förordningen (2007:854) med instruktion för Försvarets materielverk (2009:641) ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

5 §¹

Vid Försvarets materielverk finns ett nationellt certifieringsorgan för it-säkerhet i produkter och system. Materielverket, certifieringsorganet, ska i sin verksamhet beakta nationella säkerhetsintressen, verka för att uppnå och vidmakthålla internationellt erkännande för utfärdade certifikat samt vara Sveriges signatär och representant inom den internationella överenskommelsen för ömsesidigt erkännande av certifikat (CCRA) och motsvarande överenskommelse inom Europa (SOG-IS MRA).

Certifieringsorganet ska ansvara för certifiering av anordningar för skapande av kvalificerade elektroniska underskrifter och anordningar för kvalificerade elektroniska stämpelar enligt artikel 30 och 39 i Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG.

Denna förordning träder i kraft den 1 oktober 2025.

¹ Senaste lydelse 2016:577.

1.4 Förslag till förordning om ändring i förordningen (2007:951) med instruktion för Post- och telestyrelsen

Härigenom föreskrivs att 4 § i förordningen (2007:951) med instruktion för Post- och telestyrelsen ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

4 §¹

Post- och telestyrelsen har till uppgift att

1. främja tillgången till säkra och effektiva elektroniska kommunikationer, inbegripet att se till att samhällsomfattande tjänster finns tillgängliga, och att främja tillgången till ett brett urval av elektroniska kommunikationstjänster,

2. främja utbyggnaden av och följa tillgången till bredband och mobiltäckning i alla delar av landet, inbegripet att skapa förutsättningar för samverkan mellan myndigheter som kan bidra till utbyggnaden av bredband,

3. svara för att möjligheterna till radiokommunikation och andra användningar av radiovågor utnyttjas effektivt,

4. svara för att nummer ur nationella nummerplaner utnyttjas på ett effektivt sätt,

5. främja en effektiv konkurrens,

6. övervaka pris- och tjänsteutvecklingen,

7. bedriva informationsverksamhet riktad till konsumenter,

8. följa utvecklingen när det gäller säkerhet vid elektronisk kommunikation och uppkomsten av eventuella miljö- och hälsorisker,

9. pröva frågor om tillstånd och skyldigheter, fastställa och analysera marknader samt utöva tillsyn och pröva tvister enligt lagen (2022:482) om elektronisk kommunikation,

10. meddela föreskrifter enligt förordningen (2022:511) om elektronisk kommunikation,

11. upprätta och offentliggöra planer för frekvensfördelning till ledning för radioanvändningen samt offentliggöra information av allmänt intresse om rättigheter, villkor, förfaranden och avgifter som rör radiospektrumanvändningen,

¹ Senaste lydelse 2022:515.

12. tillhandahålla information om frekvensanvändning till Europeiska radiokommunikationskontorets frekvensinformationssystem (EFIS),

13. vara marknadskontrollmyndighet enligt radioutrustningslagen (2016:392),

14. vara tillsynsmyndighet enligt lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering *och* ge stöd och information till myndigheter och enskilda när det gäller betrodda tjänster,

14. vara tillsynsmyndighet enligt lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering *och utgöra gemensam kontaktpunkt för betrodda tjänster, europeiska digitala identitetsplånböcker och anmälda system för elektronisk identifiering enligt Europaparlamentets och rådets förordning (EU) 2024/1183 av den 11 april 2024 om ändring av förordning (EU) nr 910/2014 vad gäller inrättandet av ett europeiskt ramverk för digital identitet samt* ge stöd och information till myndigheter och enskilda när det gäller betrodda tjänster,

15. följa utvecklingen när det gäller toppdomäner med geografiska namn som har anknytning till Sverige,

16. vara tillsynsmyndighet enligt lagen (2006:24) om nationella toppdomäner för Sverige på internet samt meddela föreskrifter enligt förordningen (2006:25) om nationella toppdomäner för Sverige på internet,

17. verka för robusta elektroniska kommunikationer och minska risken för störningar, inbegripet att upphandla förstärkningsåtgärder, och verka för ökad krishanteringsförmåga,

18. verka för ökad nät- och informationssäkerhet i fråga om elektronisk kommunikation, genom samverkan med myndigheter som har särskilda uppgifter inom informationssäkerhets-, säkerhets-, skydds- och integritetsskyddsområdet samt med andra berörda aktörer,

19. lämna råd och stöd till myndigheter, kommuner och regioner och till företag, organisationer och andra enskilda i frågor om nät-säkerhet,

20. vara tvistlösnings- och tillsynsmyndighet enligt lagen (2016:534) om åtgärder för utbyggnad av bredbandsnät och ansvara för informationstjänsten för utbyggnad av bredbandsnät enligt samma lag, och

21. vara tillsynsmyndighet enligt lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Denna förordning träder i kraft den 1 oktober 2025.

1.5 Förslag till förordning om ändring i förordningen (2007:1110) med instruktion för Bolagsverket

Härigenom föreskrivs i fråga om förordningen (2007:1110) med instruktion för Bolagsverket att det ska införas en ny paragraf, 2 b § av följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

2 b §

Bolagsverket ska i fråga om juridiska personer ansvara för tillhandahållandet av sådana person-identifieringsuppgifter som ska kunna kopplas till den europeiska digitala identitetslånboken i enlighet med Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (EU:s förordning om elektronisk identifiering).

Denna förordning träder i kraft den 1 oktober 2025.

1.6 Förslag till förordning om ändring i offentlighets- och sekretessförordningen (2009:641)

Härigenom föreskrivs att 6 § offentlighets- och sekretessförordningen (2009:641) ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

6 §¹

Sekretess gäller i nedan angiven verksamhet, som avser registrering av betydande del av befolkningen, för

1. uppgift om en enskilds personliga förhållanden, om det av särskild anledning kan antas att den enskilde eller någon närstående till honom eller henne lider men om uppgiften röjs, och

2. uppgift i form av fotografisk bild av den enskilde, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider men.

För uppgift i en allmän handling gäller sekretessen i högst sjuttio år.

Verksamheten avser

fastighetsregistret
kommunala fastighetsregister

passregister och register över
nationella identitetskort
röstlängdsregister

Skatteverkets databas över
identitetskort för folkbokförda

i Sverige

Socialstyrelsens register över
legitimerad hälso- och sjukvårdspersonal och personal med bevis om rätt att använda yrkes titeln undersköterska

Verksamheten avser

fastighetsregistret
kommunala fastighetsregister
Myndigheten för digital förvaltnings databas över den europeiska digitala identitetsplanboken

passregister och register över
nationella identitetskort
röstlängdsregister

Skatteverkets databas över
identitetskort för folkbokförda

i Sverige

Socialstyrelsens register över
legitimerad hälso- och sjukvårdspersonal och personal med bevis om rätt att använda yrkes titeln undersköterska

¹ Senaste lydelse 2023: 297.

Statens jordbruksverks register över hund- och kattägare

Statens tjänstepensionsverks pensionsregister

Totalförsvarets plikt- och prövningsverks register över totalförsvarets personal

Transportstyrelsens vägtrafikregister.

Statens jordbruksverks register över hund- och kattägare

Statens tjänstepensionsverks pensionsregister

Totalförsvarets plikt- och prövningsverks register över totalförsvarets personal

Transportstyrelsens vägtrafikregister.

Denna förordning träder i kraft den 1 oktober 2025.

1.7 Förslag till förordning om ändring i förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning

Härigenom föreskrivs att 3 § i förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

3 §¹

Myndigheten ska

1. ansvara för den offentliga förvaltningens tillgång till infrastruktur och tjänster för elektronisk identifiering och underskrift,

2. främja användningen av elektronisk identifiering och underskrift, *och*

3. ansvara för de svenska förbindelsepunkterna (noderna) för gränsöverskridande elektronisk identifiering i enlighet med Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (eIDAS-förordningen) samt rättsakter som har meddelats med stöd av förordningen

2. främja användningen av elektronisk identifiering och underskrift,

3. ansvara för de svenska förbindelsepunkterna (noderna) för gränsöverskridande elektronisk identifiering i enlighet med Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (eIDAS-förordningen) samt rättsakter som har meddelats med stöd av förordningen, *och*

4. *ansvara för tillhandahållandet av en europeisk digital identitetsplånbok i enlighet med eIDAS-förordningen samt, i fråga om fysiska personer, även tillhandahålla sådana uppgifter för personidentifiering som avses i*

¹ Senaste lydelse 2023:712.

*artikel 3 i eIDAS-förordningen
vilka ska kunna kopplas till den
europeiska digitala identitetsplån-
boken.*

Denna förordning träder i kraft den 1 oktober 2025.

2 Utredningens uppdrag och arbete

2.1 Utredningens uppdrag

Regeringen beslutade den 22 december 2022 kommittédirektiv om att ge en särskild utredare i uppdrag att utreda och lämna förslag på hur staten kan utfärda en e-legitimation på högsta tillitsnivå. Utredaren ska också se över behovet av anpassningar som följer av den reviderade eIDAS-förordningen.

Av utredningsdirektiven framgår bl.a. att utredningen ska

- utreda hur det kan säkerställas att en kostnadseffektiv digital identitetsplånbok i enlighet med den reviderade eIDAS-förordningen ska utfärdas,
- utreda hur en sådan digital plånbok kan användas ändamålsenligt för största möjliga nationella effektivitet och nytta,
- ta ställning till vilken myndighet som bör utses till tillsynsorgan med ansvar för ett register över förlitande parter enligt kraven i den reviderade eIDAS-förordningen,
- analysera den slutgiltiga versionen av förordningen i sin helhet och ge förslag på hur Sverige kan uppfylla tillkommande krav,
- föreslå de författningsändringar och andra åtgärder som krävs för att den föreslagna myndigheten ska kunna vidta de åtgärder som åläggs den enligt förordningen, samt
- lämna de författningsförslag i övrigt som är nödvändiga eller annars bedöms lämpliga för att komplettera förordningen.

Utredningens direktiv finns bifogade till betänkandet i bilaga 1.

2.2 Utredningens arbete

Utredningsarbetet påbörjades i januari 2023. Under utredningstiden har vi haft sex sammanträden med sakkunnig- och expertgruppen.

Utöver att ha tagit del av relevant skriftligt underlag har vi genomfört ett antal möten och samtal med både aktörer i offentlig förvaltning och utfärdare av privata e-legitimationer.

Vi har enligt våra direktiv haft att beakta relevant arbete som bedrivs inom Regeringskansliet och utredningsväsendet samt särskilt beakta det arbete som bedrivs hos Myndigheten för digital förvaltning (Digg). Vi har under utredningstiden haft flera möten och kontakter med bl.a. Bolagsverket, Digg och Post- och telestyrelsen.

Visst underlag till konsekvensutredningen har tagits fram av Governo AB på vårt uppdrag.

2.3 Utredningens prioriteringar

Den reviderade eIDAS-förordningen publicerades i Europeiska unionens officiella tidning den 30 april 2024 och trädde i kraft den 20 maj 2024 (se bilaga 2). Någon konsoliderad version av eIDAS-förordningen med de ändringar som genomförts i samband med revideringen har i skrivande stund inte publicerats.

Före den 30 april 2024 har vi fått arbeta med tillgängliga utkast. Detta har i hög utsträckning försvårat arbetet och avsaknaden av den beslutade förordningstexten under merparten av utredningstiden har lett till att det varit nödvändigt att prioritera frågor som enligt vår bedömning är de mest centrala för att skapa förutsättningar för att Sverige ska kunna följa den reviderade eIDAS-förordningen med utgångspunkt för vad som i skrivande stund är känt. Eftersom det stora antal genomförandeakter som ska komplettera förordningen inte är klara vid tidpunkten då utredningen lämnas är det inte heller möjligt att få en full överblick över förordningens tillämpning och konsekvenser.

2.4 Betänkandets disposition

I kapitel 3 definieras några för betänkandet centrala begrepp och termer.

I kapitel 4 redogörs för eIDAS-förordningen.

Kapitel 5 innehåller en redovisning av nationell reglering av elektronisk identifiering och betrodda tjänster.

Kapitel 6 innehåller utredningens överväganden och förslag.

I kapitel 7 behandlas ikraftträdande och övergångsbestämmelser.

I kapitel 8 redogör vi för konsekvenserna av våra förslag.

I kapitel 9 finns författningskommentarerna.

3 Begrepp och termer

3.1 Identitetsbeteckningar

I Sverige finns två identitetsbeteckningar för fysiska personer som används i folkbokföringsverksamheten och i samhället i övrigt: personnummer och samordningsnummer.

Personnummer är enligt 18 § folkbokföringslagen (1991:481) avsett att utgöra en identitetsbeteckning för varje folkbokförd person. Även om personen skulle avregistreras från folkbokföringen, exempelvis vid utflyttning, behåller personen sitt personnummer. Personnumret och den historiska informationen som är kopplad till detta finns kvar i folkbokföringsdatabasen. För att upprätthålla tilltron till personnumret som identifikationsbegrepp är det reserverat för personer som är folkbokförda.¹

Personer som inte är folkbokförda i Sverige kan under vissa förutsättningar tilldelas ett *samordningsnummer* av Skatteverket.² På motsvarande sätt som personnummer är samordningsnummer unika såtillvida att två identiska samordningsnummer inte förekommer. Om en person med ett samordningsnummer senare blir folkbokförd ersätts samordningsnumret med ett personnummer. Individens koppling till samordningsnumret finns emellertid kvar i registret. Den huvudsakliga regleringen av samordningsnummer finns i lagen (2022:1679) om samordningsnummer.³

Personnummer och samordningsnummer utgör inte känsliga personuppgifter i dataskyddsförordningens mening, men behandlingen av dessa uppgifter omfattas genom nationell lagstiftning av särskilda villkor (se även avsnitt 6.3.9).

¹ Se mer om personnummer i delbetänkandet *En säker och tillgänglig statlig e-legitimation* (SOU 2023:61), s. 147 ff.

² Denna identitetsbeteckning har motiverats av risken för personförväxling och behovet av en säker kommunikation mellan myndigheter, se prop. 1997/98:9 s. 78 ff.

³ Se mer om samordningsnummer i delbetänkandet *En säker och tillgänglig statlig e-legitimation* (SOU 2023:61), s. 148 ff.

Det kan här noteras att i förordning (EU) 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, här efter kallad eIDAS-förordningen, används uttrycket personidentifieringsuppgift i stället för identitetsbeteckning. Detta begrepp har i Europaparlamentets och rådets förordning (EU) 2024/1183 av den 11 april 2024 om ändring av förordning (EU) nr 910/2014 vad gäller inrättandet av ett europeiskt ramverk för digital identitet, här efter kallad den reviderade eIDAS-förordningen, fått benämningen uppgifter för personidentifiering och även delvis fått en annan innebörd.

I artikel 3.3 i den reviderade eIDAS-förordningen definieras *uppgifter för personidentifiering* som en uppsättning uppgifter som utfärdas i enlighet med unionsrätten eller nationell rätt, som gör det möjligt att fastställa identiteten på en fysisk eller juridisk person eller på en fysisk person som företräder en annan fysisk person eller en juridisk person. Det rör sig således bl.a. om identitetsbeteckningar för att identifiera en fysisk person och det kan exempelvis vara ett personnummer, samordningsnummer eller ett organisationsnummer som används för att identifiera en juridisk person. I betänkandet kommer personidentifieringsuppgifter och uppgifter för personuppgiftsidentifiering användas som synonyma begrepp med den innebörd som framgår av artikel 3.3 i den reviderade eIDAS-förordningen. I författningsförslagen används emellertid endast uppgifter för personuppgiftsidentifiering.

Organisationsnummer är en identitetsbeteckning för juridiska personer. Den myndighet som registrerar företag, föreningar eller andra organisationer när de ska bildas, tilldelar organisationsnumret. De flesta juridiska personer får sitt organisationsnummer från Bolagsverket. Organisationsnummer kan även tilldelas av bl.a. Skatteverket, Statistiska centralbyrån och Lantmäteriet. Det är Skatteverket som i enlighet med 5 § lagen (1974:174) om identitetsbeteckning för juridiska personer m.fl. för ett centralt register över tilldelade organisationsnummer.

3.2 Identifiering och autentisering

Av artikel 3.1 i den reviderade eIDAS-förordningen framgår att *elektronisk identifiering* är en process inom vilken uppgifter för person-identifiering i elektronisk form, som unikt avser en fysisk eller juridisk person eller en fysisk person som företräder en annan fysisk person eller en juridisk person, används.

I artikel 3.5 i den reviderade eIDAS-förordningen definieras *autentisering* som en elektronisk process som gör det möjligt att bekräfta en fysisk eller juridisk persons elektroniska identifiering eller att bekräfta ursprunget för och integriteten hos uppgifter i elektronisk form (jfr *validering*, avsnitt 3.6.2). Svenska datatermgruppen definierar autentisering som kontroll av uppgiven identitet, t.ex. vid inloggning, vid kommunikation mellan två system eller vid utväxling av meddelande mellan användare.⁴ Internetstiftelsen å sin sida definierar autentisering som att helt enkelt kunna visa upp och styrka sin identitet för en annan part.⁵

Det förekommer flera olika metoder av autentisering. I samband med autentisering brukar det talas om en-, två- eller flerfaktorsautentisering. Användning av lösenord eller PIN-kod brukar ses som enfaktorsautentisering som baseras på något en person vet eller kan. Med dessa metoder går det egentligen bara att veta att lösenordet och PIN-koden används, men inte av vem.

Tvåfaktorsautentisering kan vara en kombination av lösenord, dvs. något som personen kan, med något som personen har, exempelvis ett smartkort eller en applikation i en mobiltelefon, alternativt i kombination med någon form av inloggning med biometrisk avläsning, t.ex. med fingeravtryck. Även andra autentiseringslösningar kan användas såsom koddosor, USB-stickor, engångslösenord via sms m.m.

Ett annat begrepp som förekommer med koppling till autentisering är *stark autentisering*. I den reviderade eIDAS-förordningen definieras i artikel 3.51 stark användarautentisering som en autentisering som är baserad på användningen av åtminstone två autentiseringsfaktorer från olika kategorier av antingen kunskap (något som endast användaren känner till), besittning (något som endast användaren besitter) eller unik egenskap (något som användaren är) som är oberoende av varandra på ett sådant sätt att en incident avseende en

⁴ www.termado.com/DatatermSearch/?ss=autentisering (hämtad 2024-05-05).

⁵ internetstiftelsen.se/guide/digitala-identiteter/ordlista/ (hämtad 2024-03-05).

av faktorerna inte äventyrar tillförlitligheten hos de andra, och som är utformad för att skydda konfidentialiteten för autentiseringsdata.

3.3 E-legitimation

Begreppen e-legitimation och elektronisk identitetshandling förekommer inte i eIDAS-förordningen. Där används i stället *medel för elektronisk identifiering* som i artikel 3.2 i den reviderade eIDAS-förordningen definieras som en materiell och/eller immateriell enhet som innehåller uppgifter för personidentifiering och som används för autentisering för en nättjänst eller, i tillämpliga fall, för en offlinetjänst. Vad gäller författningstext är medel för elektronisk identifiering det uttryck som används både i eIDAS-förordningen och nationella författningar.

Med begreppet *e-legitimation*, som används i detta betänkande, avses en identitetshandling som kan användas för att identifiera innehavaren på elektronisk väg.⁶ Med hjälp av en e-legitimation kan innehavaren identifiera sig och myndigheter eller andra aktörer som har digitala tjänster få en bekräftelse på vem personen är. En e-legitimation innehåller, liksom en fysisk identitetshandling, uppgifter som entydigt kan kopplas till en viss person.⁷

Alla former av medel för elektronisk identifiering kan således inte anses utgöra en e-legitimation utan det krävs att det rör sig om en handling som har en både tydlig och säker koppling till innehavarens identitet. En e-legitimation kan finnas som en applikation i en mobiltelefon eller surfplatta eller som en fil på en dator. Den kan också finnas på en fysisk bärare, såsom ett smartkort. Kortet innehåller då ett chip där informationen lagras.⁸

⁶ Elektronisk identitetshandling är en alternativ benämning, om vilken det anförts att den bättre återspeglar syfte och användning, dvs. att visa respektive kontrollera en individs identitet och inte uttala något om dennes behörigheter, se *reboot – omstart för den digitala förvaltningen* (SOU 2017:114), s. 171 f. Jfr dock 2017 års ID-kortutredning som förordade den inarbetade benämningen e-legitimation, vilken bl.a. används i det tillitsramverk som Myndigheten för digital förvaltning ansvarar för och som gäller för det kvalitetsmärke som för närvarande benämns Svensk e-legitimation, se *Ett säkert statligt ID-kort – med e-legitimation* (SOU 2019:14), s. 129 f.

⁷ *Ett säkert statligt ID-kort – med e-legitimation* (SOU 2019:14), s. 129.

⁸ Ibid.

3.4 Den europeiska digitala identitetsplånboken

Enligt definitionen i artikel 3.42 i den reviderade eIDAS-förordningen är en europeisk digital identitetsplånbok ”ett medel för elektronisk identifiering som gör det möjligt för användaren att på ett säkert sätt lagra, hantera och validera personidentitetsuppgifter och elektroniska attributsintyg i syfte att tillhandahålla dem till förlitande parter och andra användare av europeiska digitala identitetsplånböcker, och att underteckna med kvalificerade elektroniska underskrifter eller att stämpla med kvalificerade elektroniska stämplor”.

För att förenklat beskriva den europeiska digitala identitetsplånboken finns behov av att ibland göra åtskillnad mellan plånbokslösning (”Wallet Solution”) och plånboksinstans (”Wallet instance”).⁹

Med *plånbokslösning* avses den mjukvara med de arkitekturval, protokoll, egenskaper och andra vägval som tillhandahållaren gjort för att möta kraven som följer av definitionen och regleringen i den reviderade eIDAS-förordningen. En plånbokslösning ska certifieras som en europeisk digital identitetsplånbok innan den får tillhandahållas till fysiska och juridiska personer. Därefter kan plånbokslösningen hämtas och installeras som en lokal kopia på en mobiltelefon eller till en annan terminal, dvs. en *plånboksinstans*. När uppgifter för personidentifiering (PID) kopplats till plånboksinstansen är den giltig och utgör en europeisk digital identitetsplånbok. Plånboksinstansen kontrolleras av användaren och kan användas i tjänster som tillhandahålls av förlitande parter. Se mer om plånbokslösning, plånboksinstans och PID samt faserna för dessa i avsnitt 4.7.5.

3.5 Förlitande part

En förlitande part är enligt definitionen i artikel 3.6 i den reviderade eIDAS-förordningen ”en fysisk eller juridisk person som förlitar sig på elektronisk identifiering, europeiska digitala identitetsplånböcker eller andra medel för elektronisk identifiering eller på en betrodd tjänst”. Med andra ord är den förlitande parten exempelvis den aktör som tillhandahåller en digital tjänst där åtkomst ges efter att identifiering skett med en e-legitimation.

⁹ En sådan åtskillnad görs i *The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework Architecture and Reference Framework*, version 1.4.0.

3.6 Betrodda tjänster och de funktioner som utgör betrodda tjänster

3.6.1 Vad är betrodda tjänster?

En del av eIDAS-förordningen reglerar betrodda tjänster. Betrodda tjänster definieras i artikel 3.16 i den reviderade eIDAS-förordningen som en elektronisk tjänst som vanligen tillhandahålls mot ekonomisk ersättning och som består av en uppräkningslista i förordningen av vissa utpekade funktioner som utgör betrodda tjänster.

3.6.2 De funktioner som utgör betrodda tjänster

Förenklat kan betrodda tjänster som samlingsbegrepp, utifrån den reviderade förordningen, sammanfattas med att det är elektroniska tjänster som erbjuder vissa utpekade funktioner kopplade till elektroniska underskrifter, elektroniska stämplatser, elektroniska tidsstämplingar, elektroniskt intygande av attribut, elektronisk arkivering av elektroniska dokument, registrering av data i elektroniska liggare eller certifikat för autentisering av webbplatser. Dessutom är elektroniska tjänster för rekommenderade leveranser betrodda tjänster i sig. En närmare genomgång av dessa funktioner återfinns nedan.

Utfärdande

Utfärdande av certifikat eller av elektroniska intyg av attribut eller av elektroniska tidsstämplingar definieras inte tydligt i förordningen. Däremot framgår det att utfärdandet innebär att den som tillhandahåller tjänsten går i god för att koppla ett visst certifikat till en viss fysisk- eller juridisk person eller webbplats. Det kan även innebära att utfärdaren av ett elektroniskt intyg om ett attribut går i god för att det attributet stämmer om den fysiska eller juridiska person som attributet kopplas till. Utfärdaren kan även gå i god för att en händelse, t.ex. en elektronisk underskrift, skett vid en viss exakt tidpunkt genom en tidsstämplingstjänst.

Skapande

Funktionen skapande definieras inte i förordningen. Innebörden av skapande är däremot tämligen uppenbar enligt vår mening. Av artikel 3.22 framgår vidare att en anordning för underskriftsframställning är en konfigurerad programvara eller maskinvara som används för att skapa en elektronisk underskrift.

Validering

Funktionen validering definieras i artikel 3.41 i den reviderade eIDAS-förordningen som en process genom vilken det kontrolleras och bekräftas att data i elektronisk form är giltiga i enlighet med denna förordning. Med validering avses alltså en tjänst som kompletterar användningen av t.ex. elektroniska underskrifter och som kontrollerar att en sådan underskrift är äkta. Detaljerade bestämmelser om validering av kvalificerade elektroniska underskrifter finns i artikel 32. Av artikel 40 följer att motsvarande sätt ska gälla för validering och bevarande av kvalificerade elektroniska stämplat.

I syfte att illustrera hur valideringen av en elektronisk underskrift går till beskrivs processen nedan på ett övergripande sätt. Genom valideringen ska alla de komponenter som har använts för att skapa underskriften säkras. Detta innebär bl.a. kontroll av giltighet för certifikatet, att valideringsuppgifterna överensstämmer med de uppgifter som lämnats till den förlitande parten och att den undertecknade eller stämplade informationen inte har förändrats sedan den skrevs under. Valideringen innebär även att ett flertal olika kontroller görs för att säkerställa att en underskrift är äkta och oförvanskad. Dessa kontroller görs normalt av en intern tjänst i en organisation eller av en, kvalificerad eller icke-kvalificerad, betrodd tjänst som tillhandahålls av tredje part. Valideringstjänsten lämnar då vidare ett resultat av valideringen som är undertecknat eller stämplat av valideringstjänsten.

Kontrollen som omfattas av valideringen är att certifikatet som underskriften skapats med är utfärdat av en utfärdare som är betrodd, av den egna organisationen eller finns i förteckningen över kvalificerade tillhandahållare av kvalificerade elektroniska underskrifter. I eIDAS-förordningen finns även krav gällande kvalificerade valideringstjänster och på validering av avancerade elektroniska underskrifter skapade

med kvalificerade certifikat (artikel 33 respektive artikel 32 a i den reviderade eIDAS-förordningen).

Bevarande

Begreppet bevarande som används i artikel 3.16 i den reviderade eIDAS-förordningen definieras inte uttryckligen. Ledning för tolkning av begreppet kan hämtas från artikel 34, där det föreskrivs att en kvalificerad tjänst för bevarande av kvalificerade elektroniska underskrifter ska göra det möjligt att förlänga underskriftens tillförlitlighet utöver perioden för teknisk giltighet. Det bör noteras att innebörden av begreppet bevarande i förordningen inte överensstämmer med innebörden av begreppet i svensk arkivlagstiftning.¹⁰

Förvaltning av anordningar för underskrifter och stämplor på distans

Begreppet förvaltning som används i artikel 3.16 i den reviderade eIDAS-förordningen definieras inte. Av definitionen av tjänsten i artikel 3.23 a i den reviderade eIDAS-förordningen följer att en kvalificerad anordning för skapande av elektroniska underskrifter på distans innebär att en kvalificerad tillhandahållare av betrodda tjänster tillhandahåller en sådan anordning som genererar, förvaltar och kopierar de data som skapar den elektroniska underskriften för undertecknarens räkning. Det innebär att hanteringen är det som en sådan tjänstetillhandahållare gör för att tillhandahålla tjänsten. Mer om den betrodda tjänsten kvalificerade tjänster för förvaltning av anordningar för skapande av elektroniska underskrifter på distans finns i avsnitt 4.9.1.

¹⁰ Av 3 § tredje stycket arkivlagen (1990:782) framgår att myndigheternas arkiv ska bevaras, hållas ordnade och vårdas så att de tillgodoser rätten att ta del av allmänna handlingar, behovet av information för rättskipningen och förvaltningen, och forskningens behov.

Tillhandahållande av elektroniska tjänster för rekommenderade leveranser

Elektronisk tjänst för rekommenderad leverans definieras i förordningens artikel 3.36 som en tjänst som gör det möjligt att överföra uppgifter mellan tredje män på elektronisk väg och tillhandahåller bevis avseende de överförda uppgifternas hantering, inklusive bevis för uppgifternas sändning och mottagande, och som skyddar överförda uppgifter mot risken för förlust, stöld, skada eller otillåtna ändringar. En mer omfattande redogörelse för tjänsten finns i avsnitt 4.8.5.

Elektronisk arkivering av elektroniska uppgifter och dokument

Elektronisk arkivering definieras i artikel 3.48 i den reviderade eIDAS-förordningen som en tjänst som säkerställer mottagande, lagring, hämtning och radering av elektroniska uppgifter och dokument i syfte att säkerställa deras hållbarhet och läsbarhet samt att bevara deras integritet, konfidentialitet och ursprungsbevis under hela bevarandeperioden. Av skäl 67 i den reviderade förordningens ingress framgår att nationella arkivinstitutioner och liknande som arkiverar och bevarar kulturarvet (exempelvis Riksarkivet) oftast är styrda av nationell reglering och inte nödvändigtvis tillhandahåller betrodda tjänster i enlighet med denna förordning.

Registrering av elektroniska uppgifter i en elektronisk liggare

Elektroniska liggare definieras i artikel 3.52 i den reviderade eIDAS-förordningen som en sekvens av elektroniska dataloggar som säkerställer dataintegriteten och riktigheten i dessa loggars kronologiska ordning. Registrering i detta fall betyder att data läggs in i liggaren. Se mer elektroniska liggare i avsnitt 4.9.4.

4 EU:s förordning om elektronisk identifiering

4.1 Ramverk för gränsöverskridande elektronisk identifiering och betrodda tjänster

Sedan september 2018 tillämpas i sin helhet Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (härefter benämnd eIDAS-förordningen alternativt EU:s förordning om elektronisk identifiering).¹

Ett syfte med införandet av eIDAS-förordningen var att främja öppenhet och förtroende för onlinetjänster för att stimulera den inre marknaden. Förordningen och dess bilagor utgör, tillsammans med kommissionens antagna genomförandeakter, en EU-rättslig grund för säker och friktionsfri digital interaktion mellan fysiska personer, företag och offentliga myndigheter genom fastställande av adekvata nivåer för säkerhet för elektronisk identifiering och betrodda tjänster (se artikel 1 och skälen 1 och 2).

En förutsättning för att uppnå detta är kravet på ömsesidigt gränsöverskridande erkännande av bl.a. identifiering och underskrifter genom användning av medel för elektronisk identifiering som har anmälts av en medlemsstat till kommissionen enligt det i förordningen föreskrivna förfarandet för gränsöverskridande användning.

E-legitimationer är medel för elektronisk identifiering och vi använder oss för enkelhetens skull fortsättningsvis av benämningen e-legitimationer i möjligaste mån. Det kan dock inte uteslutas att medel

¹ Bestämmelser om elektroniska signaturer och vissa certifikattjänster fanns tidigare i Europaparlamentets och rådets direktiv 1999/93/EG av den 13 december 1999 om ett gemenskapsramverk för elektroniska signaturer. Se mer om tidigare reglering i *Vem kan man lita på? – Enkel och ändamålsenlig användning av betrodda tjänster i den offentliga förvaltningen* (SOU 2021:9) s. 76 ff.

för elektronisk identifiering omfattar även andra lösningar för autentisering än e-legitimation. Betrodda tjänster är enkelt uttryckt elektroniska tjänster som erbjuder vissa utpekade funktioner kopplade till elektroniska underskrifter, elektroniska stämplor, elektroniska tidsstämplingar eller certifikat för autentisering av webbplatser. Dessutom är elektroniska tjänster för rekommenderade leveranser betrodda tjänster i sig.

EU-regelverket kompletteras på nationell nivå i Sverige av lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering och förordningen (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering, vilka trädde i kraft den 1 juli 2016, se mer om dessa författningar i kapitel 5.

4.2 Översyn av förordningen

I enlighet med vad som föreskrivs i artikel 49 i eIDAS-förordningen har en översyn och utvärdering av förordningen gjorts av kommissionen.

Den 19 februari 2020 tillkännagav kommissionen i meddelandet *Att forma EU:s digitala framtid* att översynen av eIDAS-förordningen skulle ske utifrån målsättningen att förordningen ska

- bli mer effektiv,
- utökas i sitt tillämpningsområde för att skapa nyttor för privat sektor, och
- främja tillgången till digitala identiteter för alla européer.

I meddelandet fastslog kommissionen också inriktningen, bl.a. att individer ska ha möjligheten att kontrollera sin digitala identitet.² Samma år (juni–oktober 2020) genomfördes ett offentligt samråd.³

² https://commission.europa.eu/system/files/2020-02/communication-shaping-europes-digital-future-feb2020_en_4.pdf (hämtad 2024-05-27). En bred användning av säkra och pålitliga användarkontrollerade digitala identiteter, så att varje användare kan ha kontroll över sin online-närvaro och sina interaktioner, angavs som ett mål även i kommissionens meddelande den 9 mars 2021, *Digital kompass 2030: den europeiska vägen in i det digitala decenniet*, se <https://eur-lex.europa.eu/legal-content/SV/ALL/?uri=CELEX%3A52021DC0118> (hämtad 2024-05-27).

³ <https://digital-strategy.ec.europa.eu/en/news/digital-identity-and-trust-commission-launches-public-consultation-eidas-regulation> (hämtad 2024-05-27).

Synpunkter inhämtades även från medlemsstaterna under bilaterala och multilaterala möten och undersökningar.

De viktigaste slutsatserna från översynen och utvärderingen var att eIDAS-förordningen måste förstärkas för att ge medborgarna möjlighet att använda både offentliga och privata tjänster, och att det finns behov av att möjliggöra utfärdande och användning av gränsöverskridande elektroniska attesteringar av attribut.⁴ Bedömningen som gjordes var att s.k. ”plånböcker för digitala identiteter” är det lämpligaste instrumentet för att åstadkomma detta. På så vis kan användarna ges möjlighet att välja vilken privat tjänsteleverantör de vill dela sina attribut med utifrån aktuellt användningsfall och beroende på den säkerhet som krävs för transaktionen. Beträffande ramen för betrodda tjänster ansågs fler åtgärder vara nödvändiga för att ytterligare harmonisera vissa förfaranden kopplade till fjärridentifiering och nationell tillsyn. Med utgångspunkt i dessa slutsatser presenterade kommissionen den 3 juni 2021 ett förslag till en reviderad förordning (Europaparlamentets och rådets förordning om ändring av förordning [EU] nr 910/2014 vad gäller inrättandet av en ram för europeisk digital identitet, COM[2021] 281).⁵

Efter genomförda förhandlingar med Europaparlamentet och rådet nåddes en slutlig överenskommelse den 8 november 2023.⁶ En central del i den reviderade förordningen är regleringen av en europeisk digital identitetsplånbok, som syftar till att ge medlemsstaternas medborgare, invånare och företag tillförlitlig tillgång till offentliga och privata onlinetjänster över hela Europa.

Sedan både Europaparlamentet och rådet formellt godkänt överenskommelsen offentliggjordes den reviderade förordningen i Europeiska unionens officiella tidning den 30 april 2024, härefter den reviderade eIDAS-förordningen.⁷ I enlighet med artikel 52 i den reviderade

⁴ I den svenska språkversionen av den reviderade eIDAS-förordningen används i stället benämningen *elektroniska attributsintyg*.

⁵ eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:52021PC0281&from=EN. (hämtad 2024-05-27) Se även Regeringskansliets faktapromemoria 2020/21:FPM118 Förordning om digital identitet.

⁶ <https://digital-strategy.ec.europa.eu/sv/news/commission-welcomes-final-agreement-eu-digital-identity-wallet> (hämtad 2024-05-27) och <https://www.europarl.europa.eu/cmsdata/278103/eIDAS-4th-column-extract.pdf>. (hämtad 2024-05-27)

⁷ Europaparlamentets och rådets förordning (EU) 2024/1183 av den 11 april 2024 om ändring av förordning (EU) nr 910/2014 vad gäller inrättandet av ett europeiskt ramverk för digital identitet, https://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=OJ:L_202401183. (hämtad 2024-05-27)

eIDAS-förordningen trädde den nya förordningen därefter i kraft den tjugonde dagen efter dess offentliggörande, dvs. den 20 maj 2024.

Kravet att tillhandahålla digitala identitetsplånböcker ska uppfyllas av medlemsstaterna inom 24 månader efter ikraftträdande av genomförandeakter som fastställer de tekniska specifikationerna för identitetsplånboken och de tekniska specifikationerna för certifiering. Dessa genomförandeakter, som ska antas sex månader efter ikraftträdandet av förordningen, kommer att bygga på de specifikationer som tagits fram inom ramen för EU:s verktygslåda för digital identitet och fastställa harmoniserade villkor för införandet av identitetsplånböckerna i hela unionen (artikel 5a.1 och 5a.23 samt artikel 5c.6).

Utöver det som redan nämnts kommer genomförandeakter att antas i en stor mängd andra avseenden. Genom sannolikt direkt tillämpliga genomförandeförordningar ska det fastställas bl.a. tekniska specifikationer, förfaranden, krav eller referensstandarder för exempelvis främjandet av användares anslutning och ibruktagande ("onboarding") av den europeiska digitala identitetsplånboken (artikel 5a.24) och registrering av förlitande parter (artikel 5b.11). Vidare förutsätts genomförandeakter som fastställer t.ex. tekniska minimispecifikationer för specificering av tillitsnivåer för e-legitimationer (artikel 8.3), referensstandarder för gränsöverskridande identitetsmatchning (artikel 11a.3), och förfaranden för kontrollen av identitet och attribut som utförs av kvalificerade tillhandahållare av betrodda tjänster (artikel 24.1 c). Trots att den reviderade eIDAS-förordningen utmärks av en redan tämligen hög detaljnivå kommer förordningen, med en stor mängd direkt tillämpliga genomförandeakter, att konkretiseras ytterligare. I dagsläget innebär detta dock att det är svårt eller närmast omöjligt att få en full överblick av förordningens tillämpning och dess konsekvenser.

Även om kraven på medlemsstaterna regleras direkt genom den reviderade eIDAS-förordningen och kommande genomförandeakter, kan – som anges i våra direktiv – regeländringar eller införande av fler kompletterande bestämmelser behövas i det nationella regelverket. Vi återkommer till våra överväganden i detta avseende i kapitel 6.

4.3 Skillnader i stora drag mellan den ursprungliga och den reviderade eIDAS-förordningen

En väsentlig förändring i förhållande till gällande förordning är införandet av regleringen om den europeiska digitala identitetsplånboken (se mer om detta i avsnitt 4.7).⁸

Vidare medför den reviderade förordningen skärpningar vad gäller säkerhetsnivåer och integritetsskydd. Samtidigt har en strävan under översynen varit att ramverket ska förenkla och harmonisera skapandet och användandet av digitala identiteter. Nya och ändrade regler avser också att underlätta offentliga upphandlingsprocesser och förbättra interoperabiliteten mellan olika nationella system.

Beträffande betrodda tjänster innebär förordningen vissa ändringar av befintliga sådana tjänster såväl som införandet av fyra nya; tillhandahålla elektroniska attributsintyg, elektronisk arkivering, elektroniska liggare och förvaltning av anordningar för underskrifter och stämplat på distans. Läs mer om de nya betrodda tjänsterna i avsnitt 4.9.

Ändringar avseende redan reglerade betrodda tjänster innebär en ökad harmonisering. Det sker genom att, för flertalet artiklar om betrodda tjänster, kommissionen ges en möjlighet att ta fram genomförandeakter. Dessa ska, för det stora flertalet tjänster, tas fram senast den 21 november 2024. De generella säkerhetsreglerna för kvalificerade och icke-kvalificerade betrodda tjänster har flyttats till det s.k. NIS2-direktivet.⁹

I den reviderade förordningen införs även nya bestämmelser, vilka tillsammans med delvis uppdaterade befintliga, utgör ett ramverk för styrning. Bestämmelserna omfattar tillsyn av den europeiska digitala identitetsplånboken såväl som betrodda tjänster (se avsnitten 4.7.4 och 4.10.5). Ramverket för styrning omfattar även bestämmelser om kommunikation mellan dels olika medlemsstater, dels medlemsstaterna och kommissionen. I sistnämnda avseende föreskrivs till att börja med

⁸ I kommissionens ursprungliga förslag fanns även (i artikel 7) ett obligatorium för medlemsstaterna att anmäla ett system för elektronisk identifiering med minst en e-legitimation på den högsta tillitsnivån. Detta krav har slopats under förhandlingarna. Kravet kan emellertid möjligen sägas följa indirekt av reglerna om den europeiska digitala identitetsplånboken. Sådana identitetsplånböcker måste nå tillitsnivå hög, särskilt när det gäller kraven på identitetskontroll och verifiering, samt hantering och autentisering av medel för elektronisk identifiering (dvs. e-legitimationer), se bl.a. artikel 5a.11 och 5a.24.

⁹ Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet) (Text av betydelse för EES).

att varje medlemsstat ska utse en gemensam kontaktpunkt för betrodda tjänster, identitetsplånboken och notifierade e-legitimations-system. Dessa ska fungera som en förbindelse för gränsöverskridande kontakt tillsynsmyndigheter emellan, samt när det är lämpligt även mellan kommissionen och Europeiska unionens cybersäkerhetsbyrå samt andra berörda myndigheter inom medlemsstaten (artikel 46c).

Vidare förskrivs nu i artikel 46d att tillsynsmyndigheterna, bl.a. genom den europeiska samarbetsgruppen för digital identitet, får söka ömsesidigt bistånd. Sådant bistånd kan sökas från en tillsynsmyndighet i en annan medlemsstat där en berörd tillhandahållare av betrodda tjänster eller tillhandahållare av en europeisk digital identitetsplånbok är etablerad, har sina nätverk och informationssystem, eller erbjuder sina tjänster. Syftet är att underlätta tillsyn och upprätthållande av regelverket i förordningen.

Nämnda samarbetsgrupp ska etableras av kommissionen för att ge stöd till och underlätta medlemsstaternas gränsöverskridande samarbete och informationsutbyte kopplat till betrodda tjänster, den europeiska digitala identitetsplånboken och notifierade system för elektronisk identifiering. Samarbetsgruppen ska bestå av representanter utnämnda av medlemsstaterna och kommissionen. Kommissionen ska agera ordförande och administrera ett sekretariat (artikel 46e).

4.4 Den reviderade förordningens struktur och innehåll

Förordningen är indelad i sju kapitel och kompletteras av sju bilagor. Kapitel I innehåller alltjämt allmänna bestämmelser. Kapitel II är nu uppdelat i två avsnitt, där det första innehåller bestämmelser om den europeiska digitala identitetsplånboken, medan det andra avsnittet handlar om system för elektronisk identifiering. I likhet med tidigare finns i kapitel III bestämmelser om betrodda tjänster. I nya kapitel IVa finns nya och delvis ändrade bestämmelser om tillsyn, vilka gemensamt utgör ett ramverk för styrning. De återstående kapitlen, kapitel IV, V och VI innehåller bl.a. bestämmelser om rättslig verkan av elektroniska dokument, delegering av befogenheter och genomförandebestämmelser samt övergångsbestämmelser och ikraftträdande.

I de följande avsnitten redogörs för den reviderade eIDAS-förordningens centrala bestämmelser och sådana bestämmelser som är av betydelse med hänsyn till utredningens uppdrag.

4.5 Allmänna bestämmelser

4.5.1 Syften

I artikel 1 i förordningen anges dess syfte. Enligt den ursprungliga lydelsen är målet med förordningen att säkerställa en väl fungerande inre marknad och uppnå en lämplig säkerhetsnivå för e-legitimationer ("medel för elektronisk identifiering") och betrodda tjänster.

I skäl 2 till förordningen i dess tidigare lydelse angavs att den syftar till att öka förtroendet för elektroniska transaktioner på den inre marknaden genom att tillhandahålla en gemensam grund för ett säkert elektroniskt samspel mellan medborgare, företag och offentliga myndigheter. Därigenom ska effektiviteten öka hos offentliga och privata nättjänster samt i elektronisk affärsverksamhet och e-handel i unionen.

I den reviderade förordningen framhålls även syftet att möjliggöra och underlätta fysiska och juridiska personers utövande av rätten att delta i det digitala samhället på ett säkert sätt och ha tillgång till offentliga och privata nättjänster i hela unionen (artikel 1.1). För dessa syften fastställer förordningen villkor för medlemsstaterna att, utöver de nuvarande, tillhandahålla och erkänna europeiska digitala identitetsplånböcker (artikel 1.1 a). I ingressen till den reviderade förordningen tydliggörs i flera punkter (skäl) att ramverket ämnar leda till en bred användning av en tillförlitlig, frivillig och användarvänlig digital identitet, se t.ex. skälen 3–6. När det talas om rätten till användning av bl.a. digitala tjänster innefattar det ett krav på medlemsstaterna att säkerställa att "alla människor i EU", dvs. unionsmedborgare och invånare i unionen (enligt definitionen i nationell rätt), men även företag erbjuds en tillgänglig, säker och tillförlitlig digital identitet som möjliggör tillgång till sådana tjänster (se t.ex. skälen 4–7).

4.5.2 Tillämpningsområde

Enligt artikel 2.1 (i dess tidigare lydelse) ska förordningen tillämpas på system för elektronisk identifiering som anmälts av en medlemsstat, och tillhandahållare av betrodda tjänster.

System för elektronisk identifiering är ett sådant system genom vilket medel för elektronisk identifiering (i detta betänkande även benämnt e-legitimationer) utfärdas till en fysisk eller juridisk person eller en fysisk person som företräder en annan fysisk person eller en juridisk person (se definitionen i dess nya lydelse i artikel 3.4). I det följande kallar vi dessa system för e-legitimationssystem för att inte göra texten onödigt svårläst.

I likhet med tidigare gäller förordningen enbart för sådana e-legitimationssystem som har anmälts till kommissionen för gränsöverskridande användning och för sådana tillhandahållare av betrodda tjänster som är etablerade inom unionen.

Med inrättandet av den europeiska digitala identitetsplånboken utvidgas tillämpningsområdet till att även omfatta identitetsplånböcker som tillhandahålls i medlemsstaterna. Förordningens tillämpning i detta avseende görs, till skillnad mot e-legitimationer, inte beroende av något anmälningsförfarande, eller annat villkor än att identitetsplånboken ska vara tillhandahållen av en medlemsstat. Reglerna om den europeiska digitala identitetsplånboken är alltså direkt tillämpliga såväl vid nationell som vid gränsöverskridande användning. Nationell reglering om den europeiska digitala identitetsplånboken är därmed tillåten bara i de delar förordningen påbjuder eller tillåter det.

I detta sammanhang bör också tilläggas att i de fall en medlemsstat kräver elektronisk identifiering och autentisering för åtkomst till digitala tjänster inom offentlig sektor ska sådana identitetsplånböcker som tillhandahållits i enlighet med den reviderade eIDAS-förordningen accepteras (artikel 5f.1). En motsvarande skyldighet ska under vissa förhållanden även gälla för privata förlitande parter när dessa till följd av bestämmelser i nationell eller unionsrättslig lagstiftning är ålagda att använda stark användarautentisering, eller om sådan krävs enligt avtalsförpliktelser (artikel 5f.2). Oaktat denna artikels rubrik, ”Gränsöverskridande användning av europeiska digitala identitetsplånböcker”, får bestämmelserna däri ses som förtydliganden, såsom att förlitande parter i privat sektor inte är skyldiga att acceptera sådana identitetsplånböcker utöver det som följer av punkten 2. Skyldig-

heter och krav enligt dessa bestämmelser kan dock inte anses gälla bara vid gränsöverskridande användning.

Utanför tillämpningsområdet ligger fortfarande sådant tillhanda-hållande av betrodda tjänster som till följd av nationell lagstiftning eller avtal mellan en avgränsad krets deltagare endast används inom slutna system (artikel 2.2).

Med vissa förtydliganden innebär vidare tillämpningsbestämmelserna att förordningen inte påverkar regler i nationell lagstiftning eller unionsrätt som avser ingående av avtal och deras giltighet, eller andra rättsliga eller förfarandemässiga skyldigheter avseende form, eller sektorspecifika krav avseende form (artikel 2.3). I skäl 46 i den reviderade förordningens ingress anges att den inte heller avser inverka på nationella formkrav avseende offentliga register, i synnerhet inte kommersiella register eller fastighetsregister.

Likaså tydliggörs genom ett tillägg i den nya punkten 4 i artikel 2 att den reviderade förordningen inte påverkar tillämpningen av Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), härefter benämnd EU:s dataskyddsförordning.¹⁰

4.5.3 Definitioner

I eIDAS-förordningen definieras en rad begrepp och uttryck i artikel 3. Mer eller mindre omfattande ändringar har gjorts i flera av definitionerna (led 1–6, 14, 16, 18, 21, 38 och 41) i den reviderade förordningen. Dessutom införs definitioner för ytterligare 19 begrepp och uttryck, t.ex. användare (led 5a), samt kvalificerad anordning för skapande av elektroniska underskrifter, respektive stämplor, på distans (led 23a och 23b, se mer om detta i avsnitt 4.9.1).

Tillkomna och ändrade definitioner behövs med anledning av bl.a. regleringen av den europeiska digitala identitetsplånboken (se särskilt led 16 och 42–57).

¹⁰ Jfr artikel 5.1 i eIDAS-förordningen i dess tidigare lydelse, som hänvisade till det numera upphävda dataskyddsdirektivet, Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.

4.5.4 Inre marknadsprincipen

Principen om en inre marknad, som slås fast i artikel 4, har inte ändrats. I likhet med tidigare får således den som tillhandahåller betrodda tjänster i en medlemsstat inte hindras att göra detta även i en annan medlemsstat av skäl som omfattas av områden som regleras i förordningen. Produkter och betrodda tjänster som överensstämmer med förordningen ska omfattas av fri rörlighet på den inre marknaden. Genom ömsesidigt erkännande av e-legitimationer ("medel för elektronisk identifiering") ska tillhandahållandet av tjänster över gränserna på den inre marknaden underlättas (se vidare avsnitt 4.6.1).

4.5.5 Användning av pseudonymer vid elektroniska transaktioner

I likhet med det som föreskrivs i den ursprungliga lydelsen av förordningen ska användning av pseudonymer vid elektroniska transaktioner inte förbjudas (artikel 5). Bestämmelsen har kompletterats såtillvida att det rör pseudonymer "som valts av användaren". Fortfarande gäller att bestämmelsen i sig inte påverkar den rättsliga verkan som pseudonymer har enligt nationell rätt. Därutöver har förtydligats att bestämmelsen inte heller påverkar tillämpningen av specifika unionsrättsliga eller nationella regler som föreskriver att användare ska identifiera sig. För att skapa tillit till de europeiska digitala identitetsplånböckerna är det nödvändigt att det kan säkerställas att den person som gör anspråk på eller hävdar en viss identitet faktiskt är den person som han eller hon utger sig för att vara. Behovet av att kunna lita på rättsligt fastställda identiteter, som regleras nationellt i varje medlemsstat, bör dock inte hindra användare av identitetsplånböcker från att få tillgång till tjänster genom användning av pseudonymer. Som framgår av skäl 19 gäller detta dock under förutsättning att det inte finns något föreskrivet krav om att uppge sin faktiska, rättsligt fastställda, identitet för att identifiera sig. Sådana krav kan uppställas i såväl unionsrätten som i medlemsstaternas nationella lagstiftning.

4.6 Elektronisk identifiering

4.6.1 Ömsesidigt erkännande

Enligt artikel 6 i eIDAS-förordningen, som inte är ändrad, ska medel för elektronisk identifiering under vissa förutsättningar omfattas av ömsesidigt erkännande. Det gäller sådana e-legitimationer som är utfärdade inom ramen för ett e-legitimationssystem som har anmälts av en medlemsstat och förts upp på en särskild förteckning som offentliggörs av kommissionen (se mer om anmälningsförfarandet i nästa avsnitt).

Det kan i sammanhanget noteras att en innehavare inte alltid har möjlighet att använda tillhandahållna nättjänster efter genomförd inloggning, trots kravet på ömsesidigt erkännande av anmälda e-legitimationer. I dagsläget är det vanligt att den som använt en utländsk e-legitimation hamnar i ett s.k. digitalt väntrum, där det inte går att utföra det förfarande som tjänsten avser. Detta är en följd av att många digitala tjänster inom den offentliga förvaltningen ställer krav på användning av exempelvis personnummer (se även avsnitt 4.6.4).

4.6.2 Anmälningsförfarande och tillitsnivåer

Liksom tidigare är det endast medlemsstater som kan anmäla e-legitimationssystem, och det behöver inte vara medlemsstaten som utfärdar e-legitimationerna i systemet. E-legitimationerna kan vara utfärdade av den anmälande medlemsstaten, på uppdrag av den anmälande medlemsstaten eller oberoende av den anmälande medlemsstaten men erkännas av medlemsstaten.

En anmälan delas in i tre steg. Det första steget är s.k. föransökan. Under detta steg förser den anmälande medlemsstaten andra medlemsstater med information om det system som anmäls. Nästa steg är enligt vedertagen praxis en sakkunnigbedömning. Under detta steg bedöms kvaliteten och säkerheten i det anmälda systemet utifrån kraven i förordningen och genomförandeförordning (EU) 2015/1502.¹¹ Bedömningen genomförs av andra medlemsstater och avslutas

¹¹ Kommissionens genomförandeförordning (EU) 2015/1502 av den 8 september 2015 om fastställande av tekniska minimispecifikationer och förfaranden för tillitsnivåer för medel för elektronisk identifiering i enlighet med artikel 8.3 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden.

med ett utlåtande som antas av samtliga medlemsstater. Det sista steget är formell anmälan och publicering i EU:s officiella tidning.¹²

De krav som måste vara uppfyllda för att anmäla ett e-legitimationssystem framgår av artikel 7. Av artikel 9 följer vilka uppgifter som en anmälan ska innehålla och i artikel 8 finns bestämmelser (kompletterade genom tidigare nämnd genomförandeförordning) om tillitsnivåer för e-legitimationssystem. Tillitsnivåerna återger graden av tillit till en e-legitimation vid fastställande av en persons identitet och skapar visshet om att den person som gör anspråk på en viss identitet faktiskt är den person som har tilldelats denna identitet.

Som redan nämnts innebar rådets förslag till reviderad förordning en uttrycklig skyldighet för medlemsstaterna att anmäla ett e-legitimationssystem med åtminstone en e-legitimation på högsta tillitsnivå (se avsnitt 4.3). Indirekt gäller dock ett sådant krav eftersom minst en europeisk digital identitetsplånbok ska tillhandahållas av varje medlemsstat inom ramen för ett system för elektronisk identifiering (artikel 5a.1, 5a.5 f och 5a.24). Till dess att en eventuell genomförandekt enligt artikel 5a.24 har antagits krävs identifiering med en e-legitimation på tillitsnivå hög för att få tillgång till en identitetsplånbok.

I artiklarna 7–9 återstår nu enbart vissa redaktionella ändringar (artikel 7 g, artikel 8.3, artikel 9.2 och artikel 9.3).

Sakkunnighetsbedömningen av anmälda e-legitimationssystem har, som nämnts, vuxit fram som en praxis mellan medlemsstaterna med beaktande av föreskriven samarbetskyldighet i artikel 12.5 i dess tidigare lydelse. Sakkunnighetsbedömningen av e-legitimationssystem görs obligatorisk genom en ändrad lydelse av artikel 12.5 och dess hänvisning till artikel 9.1 a. Anmälningsförfarandet påverkas således av denna ändring samt av bestämmelser i den nya artikeln 12a (se vidare avsnitt 4.6.6, jfr 4.7.5).

4.6.3 Säkerhetsincidenter och skadeståndsansvar

I artikel 10 i eIDAS-förordningen finns bestämmelser om hantering av säkerhetsincidenter i anmälda e-legitimationssystem eller den autentisering som avses i artikel 7 f. Vid intrång eller om systemet äventyras

¹² Sverige har tre e-legitimationer som är föranmälda och granskade av andra medlemsstater. En av dessa e-legitimationer, Freja+, är anmäld och kan därmed användas för gränsöverskridande e-legitimering inom EU. <https://ec.europa.eu/digital-building-blocks/sites/display/EIDCOMMUNITY/Sweden> (hämtad 2024-05-26)

på ett sätt som påverkar tillförlitligheten i dess gränsöverskridande autentisering ska den anmälade medlemsstaten utan dröjsmål tillfälligt upphäva eller återkalla denna gränsöverskridande autentisering eller de berörda utsatta delarna. Artikel 11 fastslår även när sådan autentisering ska återinföras samt informationsskyldighet för berörd medlemsstat och kommissionen med anledning av en säkerhetsincident. I den reviderade förordningen görs inga förändringar av artikeln, vars rubrik dock förtydligas för att tydliggöra att artikeln reglerar incidenter i e-legitimationssystem (säkerhetsincidenter och informationskrav i fråga om digitala identitetsplånböcker regleras i artikel 5e i den reviderade eIDAS-förordningen).

Bestämmelser om skadeståndsansvar finns i artikel 11, som gäller för den anmälade medlemsstaten, den som har utfärdat e-legitimationer och den part som har hand om autentiseringsförfarandet, ifall dessa inte uppfyller sina skyldigheter enligt förordningen. Bestämmelserna är desamma i den reviderade förordningen.

4.6.4 Gränsöverskridande identitetsmatchning

I den reviderade förordningen föreskrivs att medlemsländerna ska säkerställa otvetydig identitetsmatchning för gränsöverskridande tjänster (artikel 11a.1).¹³ Skyldigheten gäller för medlemsstater i egenskap av förlitande parter, dvs. den träffar offentliga aktörers digitala tjänster.

Identitetsmatchning definieras som ”en process där uppgifter för personidentifiering eller medel för elektronisk identifiering matchas mot eller kopplas till ett befintligt konto som tillhör samma person” (artikel 3.55).

I den reviderade eIDAS-förordningen anges att offentliga aktörer använder de personidentifieringsuppgifter som finns tillgängliga i systemen för e-legitimationer för att matcha den elektroniska identiteten hos användare från andra medlemsstater med de personidentifieringsuppgifter som tillhandahålls dessa användare i den medlemsstat som utför den gränsöverskridande identitetsmatchningsprocessen. Vidare konstateras att det, trots användningen av förordningens föreskrivna

¹³ I kommissionens förslag till reviderad förordning innehöll artikel 11a en skyldighet för medlemsstaterna att, i fråga om anmälda e-legitimationer och digitala identitetsplånböcker, säkerställa en unik identifiering (”unique identification”) genom att i minimiuppsättningen av personidentifieringsuppgifter inkludera en unik och beständig identifierare (”unique and persistent identifier”), eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:52021PC0281&from=EN (hämtad 2024-05-27).

minimiuppsättning av sådana uppgifter, krävs ytterligare information om användaren och särskilda kompletterande unika identifieringsförfaranden som ska utföras på nationell nivå för att säkerställa korrekt identitetsmatchning när medlemsstaterna agerar som förlitande parter (skäl 41).

Det nya kravet på gränsöverskridande identitetsmatchning avser enligt skäl 41 vidare att ytterligare stödja användbarheten av e-legitimationer, tillhandahålla bättre offentliga nättjänster och öka rättssäkerheten när det gäller användarnas elektroniska identitet.

För att säkerställa en hög skyddsnivå för personuppgifter som används för identitetsmatchning och för att förhindra profilering av användare ska medlemsstaterna se till att det finns tekniska och organisatoriska förutsättningar för detta (artikel 11a.2). Referensstandarder samt, vid behov, specifikationer och förfaranden för den före skrivna identitetsmatchningen ska fastställas av kommissionen i en genomförandeakt (artikel 11a.3).

4.6.5 Interoperabilitet

Enligt artikel 12 i eIDAS-förordningen ska nationella e-legitimationssystem som anmälts för gränsöverskridande användning enligt artikel 9.1 vara interoperabla. För tillämpningen av detta krav finns ett fastställt interoperabilitetsramverk (artikel 12.3–6 med tillhörande genomförandeakter).

Den reviderade förordningen innebär en ökad betydelse av interoperabilitet, som också utgör ny rubrik för artikeln. I stället för nuvarande krav på medlemsstaterna att samarbeta kring interoperabilitet och säkerhet, ska de genomföra sakkunnighetsbedömningar av anmälda e-legitimationssystem. I likhet med tidigare kommer närmare reglering av sådana granskningar att fastställas av kommissionen i genomförandeakter (artikel 12.6 och 12.8).

Vidare görs vissa förtydliganden och kompletteringar, bl.a. fastslås att ramverket ska främja tillämpning av inte bara principen om ett inbyggt integritetsskydd utan även inbyggt säkerhet (artikel 12.3 c).

4.6.6 Certifiering av e-legitimationssystem

I den reviderade eIDAS-förordningen införs, såvitt gäller e-legitimationssystem, bestämmelser om certifiering i en ny artikel 12a (se även artikel 5c avseende certifieringskrav för den digitala identitetsplånboken).

Medlemsstaterna ska utse organ med uppgift att certifiera att system för elektronisk identifiering som ska genomgå det tidigare redovisade anmälningsförfarandet överensstämmer med de krav på cybersäkerhet som föreskrivs i förordningen.

Vidare fastslås att denna certifiering ska utföras inom ramen för en relevant ordning för cybersäkerhetscertifiering enligt förordning (EU) 2019/881¹⁴ eller delar därav (jfr skäl 25). Detta hindrar inte medlemsstaterna att, av den anmälade medlemsstaten, begära ytterligare information om hela eller delar av e-legitimationssystem som certifierats enligt hänvisad ordning (artikel 12a.4).

Certifieringen är giltig i högst fem år, under förutsättning att en regelbunden tvåårig sårbarhetsanalys genomförs. Om sårbarheter identifieras och inte åtgärdas inom tre månader ska certifieringen upphävas (artikel 12a.3).

Sakkunnigbedömningar som Den europeiska samarbetsgruppen för digital identitet (EDICG) får genomföra (se artikel 46e.5 d) ska inte tillämpas i fråga om system för elektronisk identifiering eller delar av sådana system som certifierats i enlighet med artikel 12a. Medlemsstaterna får använda sig av ett certifikat eller en försäkran om överensstämmelse, som utfärdats i enlighet med en relevant europeisk ordning för cybersäkerhetscertifiering eller delar av en sådan ordning beträffande krav i artikel 8.2 (tillitsnivåer) som inte avser cybersäkerhet.

4.6.7 Åtkomst till hård- och mjukvarufunktioner

Enligt nya bestämmelser i den reviderade eIDAS-förordningen ska tillhandahållare av europeiska digitala identitetsplånböcker och utfärdare av anmälda e-legitimationer under vissa angivna förutsättningar ges åtkomst till hård- och mjukvarufunktioner (artikel 12b).

¹⁴ Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten).

För att säkerställa att de digitala identitetsplånböckerna fungerar effektivt är tillhandahållarna av dessa i behov av en effektiv interoperabilitet samt rättvisa, rimliga och icke-diskriminerande villkor så att identitetsplånböckerna har tillgång till specifika maskinvaru- och programvarufunktioner i mobila enheter. I skäl 49 i förordningens ingress anges att det kan handla om tillgång till exempelvis antenner för närfältskommunikation (NFC) och säkerhetskomponenter, inbegripet universella smartkort, inbäddade säkerhetskomponenter, microSD-kort och Bluetooth Low Energy. I nämnda skäl anges vidare att tillgången till dessa komponenter kan kontrolleras av mobilnätoperatörer och utrustningstillverkare, varför tillverkare av originalutrustning för mobila enheter eller tillhandahållare av elektroniska kommunikationstjänster inte bör få neka tillgång till sådana komponenter när de behövs för att tillhandahålla tjänster relaterade till de europeiska digitala identitetsplånböckerna.

Bestämmelsen i artikel 12b omfattar specifikt sådana företag som av kommissionen utses till s.k. grindvakter för uppräknade centrala plattformstjänster enligt EU:s förordning om öppna och rättvisa marknader inom den digitala sektorn (DMA-förordningen).¹⁵ Dessa grindvakter ska således, kostnadsfritt, möjliggöra effektiv driftskompatibilitet med och, i driftskompatibilitetssyfte, ge tillgång till funktioner i operativsystem, maskinvara eller programvara, oavsett huruvida dessa funktioner är en del av det operativsystem som grindvakten har tillgång till eller använder när denne tillhandahåller sådana tjänster (i den mening som avses i artikel 6.7 i DMA-förordningen).

4.7 Europeisk digital identitetsplånbok

4.7.1 Summarisk introduktion

Syftet med att införa en europeisk digital identitetsplånbok är att se till att alla fysiska och juridiska personer inom EU på ett säkert, tillitsbaserat och sömlöst sätt ges tillgång till publika och privata tjänster inom unionen (se artikel 5a.1).

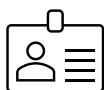
Utfärdandet, användningen och återkallandet av europeiska digitala identitetsplånböcker ska vara utan kostnad för alla fysiska personer

¹⁵ Europaparlamentets och rådets förordning (EU) 2022/1925 av den 14 september 2022 om öppna och rättvisa marknader inom den digitala sektorn och om ändring av direktiv (EU) 2019/1937 och (EU) 2020/1828 (förordningen om digitala marknader).

(se artikel 5a.13). Det ska vara frivilligt att använda identitetsplånboken och avsaknaden av en sådan ska inte påverka tillgången till service eller möjligheten att bedriva verksamhet (se artikel 5a.15). Identitetsplånboken ska, i enlighet med bestämmelserna i EU:s direktiv 2019/882, göras tillgänglig för personer med funktionsnedsättning på lika villkor (se artikel 5a.21).

Genom sin europeiska digitala identitetsplånbok ska användaren kunna begära, erhålla, välja, kombinera, lagra, radera, dela och visa uppgifter för personidentifiering (se mer om personidentifieringsuppgifter i avsnitt 4.7.4 och 6.3.3). Med ifrågavarande personidentifieringsuppgifter, och i tillämpliga fall i kombination med elektroniska attributsintyg, ska användaren kunna autentisera gentemot förlitande parter online och, när det är lämpligt, i offlineläge, i syfte att få tillgång till offentliga och privata tjänster (se artikel 5a.4 a).

Figur 4.1 Identitetsplånbokens huvudsakliga användningsområden



Identifiering/Autentisering

Förmedla uppgifter för personidentifiering som krävs för att få tillgång till offentlig och privat service hos förlitande parter.



Lagra & visa upp attributsintyg

Exempelvis studieintyg eller yrkeslegitimation för ansökan om utbildning eller arbete, eller intyg för företag om erforderliga tillstånd att driva reglerad verksamhet.



Underteckna elektroniskt

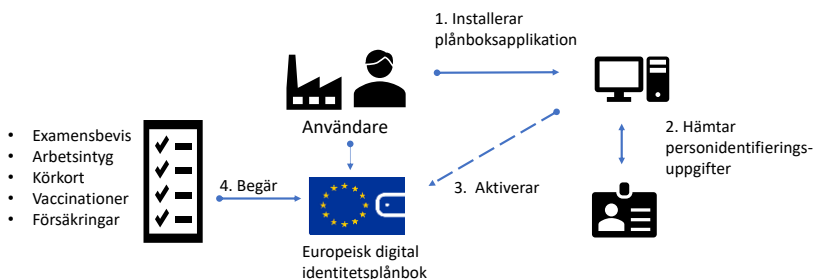
Exempelvis underteckna ett anställningskontrakt/avtal eller godkänna betalning.

Anskaffandet av en europeisk digital identitetsplånbok sker, förenklat beskrivet, genom att användaren först skaffar en digital identitetsplånbok som stöds av medlemsstaten. Därefter kopplas, med en e-legitimation på tillitsnivå hög, nödvändiga och tillräckligt säkra uppgifter för personidentifiering till den digitala plånboken (se mer om tillhandahållandet i avsnitt 6.3.1). När en sådan koppling skapats har användaren tillgång till en europeisk digital identitetsplånbok. Användaren kan därefter förse sitt exemplar av den europeiska identitetsplånboken (sin identitetsplånboksinstans) med olika attributsintyg. Med attribut avses enligt den reviderade eIDAS-förordningens definition egenska-

per, kvaliteter, rättigheter eller tillstånd hos en fysisk eller juridisk person eller hos ett föremål (se artikel 3.43). Det kan vara fråga om exempelvis studieintyg eller intyg om körkortsbehörighet. Enligt den reviderade eIDAS-förordningen ska medlemsstaterna säkerställa att identitetsplånboken – om användaren vill – kan innehålla åtminstone uppgifter om innehavarens adress, ålder, kön, civilstatus, familjesammansättning, nationalitet eller medborgarskap, utbildnings- och yrkeskvalifikationer jämte eventuella titlar och licenser, fullmakter, offentliga tillstånd och licenser samt – för juridiska personer – även finansiella data och bolagsdata (se artikel 45e och bilaga VI). Identitetsplånboken ska sedan kunna användas i såväl digitala som analoga tjänster.

Figur 4.2 illustrerar på ett förenklat sätt hur flödet vid anskaffandet av en europeisk digital identitetsplånbok ser ut.

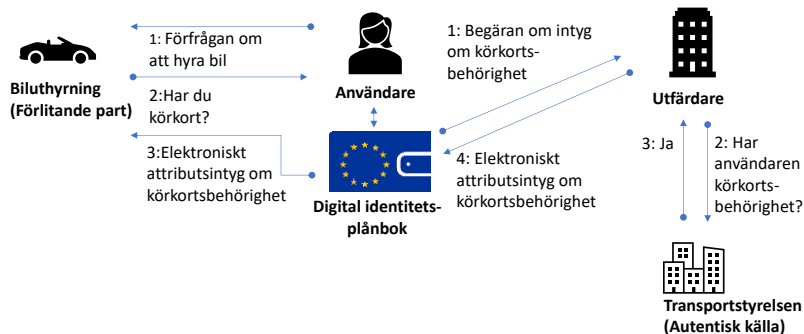
Figur 4.2 Flödet vid anskaffande av identitetsplånboken



Ett exempel på hur användaren kan ha nytta av sin identitetsplånbok i praktiken är för att visa upp sitt körkort vid bilhyra. Ett biluthyrningsföretag kräver i det sammanhanget vanligen ett intyg på att användaren innehar körkort. Användaren kan vid uthyrningstillfället, eller i förväg, via identitetsplånboken begära att ett körkortsintyg utfärdas till identitetsplånboken. Utfärdaren kan vara en extern part som vänder sig till en autentisk källa (som för körkort är Transportstyrelsen, se mer om autentiska källor i avsnitt 4.7.4) för kontroll av attributet eller till den autentiska källan direkt. Informationen kan därefter skickas till identitetsplånboksinstansen och visas upp för biluthyraren.

Figur 4.3 illustrerar användning av identitetsplånboken vid bilhyra.

Figur 4.3 Användning av identitetsplånboken vid biluthyrning



Kontroll av attribut mot autentiska källor regleras i artikel 45e. Vid utredningens kontakter med berörda intressenter har framförts att bestämmelsen kan tolkas på olika sätt i fråga om det endast är den autentiska källan som kan utfärda ett attributsintyg från en sådan källa eller inte. Vi har bedömt att bestämmelsen lämnar utrymme för i figur 4.3 beskriven ordning. Det bör dock anmärkas att bestämmelsen omfattas av kommande genomförandeförordningar vilket alltså inte har kunnat beaktas inom ramen för utredningens bedömning.

Identitetsplånboken ska erbjuda flertalet ytterligare funktioner. Det ska exempelvis vara möjligt för användaren att generera pseudonymer och lagra dem i krypterad form lokalt i identitetsplånboken, autentisera en annan persons europeiska digitala identitetsplånbok samt ta emot och dela personidentifieringsuppgifter och elektroniska attributsintyg på ett säkert sätt mellan två europeiska digitala identitetsplånböcker. Via en instrumentpanel i identitetsplånboken ska användaren ges tillgång till en logg över alla transaktioner som skett, kunna se en uppdaterad förteckning över förlitande parter med vilka användaren har upprättat en förbindelse och i tillämpliga fall alla utbytta uppgifter samt kunna begära att en förlitande part raderar personuppgifter eller rapportera en förlitande part till integritetskyddsmyndigheten vid misstanke om olagliga eller obehöriga förfrågningar (jfr artikel 5a.4 b–d).

4.7.2 En verktyglåda med en teknisk arkitektur- och referensram arbetas fram

Den 3 juni 2021 antog EU-kommissionen en rekommendation med uppmaning till medlemsstaterna att ta fram en s.k. verktyglåda inklusive en teknisk arkitektur- och referensram, vars engelska akronym är ARF (Architecture and Reference Framework).¹⁶

Verktyglådan ska innehålla en uppsättning gemensamma standarder och tekniska specifikationer samt en uppsättning gemensamma riktlinjer och bästa praxis. Enligt rekommendationen från kommissionen ska arbetet ligga till grund för genomförandet av den reviderade eIDAS-förordningen när den trätt i kraft, utan att påverka eller föregripa lagstiftningsprocessen. Verktyglådan ska komplettera den reviderade eIDAS-förordningen och möjliggöra skapandet av en robust ram för digital identifiering och autentisering som bygger på gemensamma standarder i hela EU.¹⁷ Verktyglådan utgör emellertid inte någon rättskälla utan det är endast den reviderade eIDAS-förordningen och genomförandeakterna som ska betraktas som sådana.

Arbetet med att ta fram verktyglådan sker kontinuerligt i eIDAS-expertgrupp¹⁸, som bildades i samband med antagandet av eIDAS-förordningen för att förbereda genomförandeakter enligt förordningen. Gruppen består av experter som nominerats av de olika medlemsländerna i EU/EES. Sverige har nominerat experter från flera myndigheter, bl.a. Digg, PTS, Transportstyrelsen och Polisen. I den senare delen av gruppens arbete har även deltagare från de storskaliga pilotprojekten bjudits in (se mer om pilotprojekten i avsnitt 4.7.3. nedan). Det har medfört ett ökat svenskt deltagande från främst Bolagsverket, men även Vetenskapsrådet/Sunet. Den senaste versionen av ARF:en publicerades den 23 maj och utgör version 1.4.0.¹⁹

¹⁶ COMMISSION RECOMMENDATION of 3.6.2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework.

¹⁷ <https://digital-strategy.ec.europa.eu/sv/policies/eudi-wallet-toolbox> (hämtad 2024-05-19).

¹⁸ eIDAS Expert Group (E 03032) <https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupID=3032> (hämtad 2024-05-27).

¹⁹ <https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/latest/arf/> (hämtad 2024-05-27).

4.7.3 Fyra pilotprojekt för att testa den digitala europeiska identitetsplånboken

EU-kommissionen har utlyst s.k. storskaliga pilotprojekt i syfte att testa den europeiska digitala identitetsplånboken och säkerställa att den införs på ett säkert och smidigt sätt. Pilotprojekten, som är fyra till antalet, inleddes i maj 2023 och planeras pågå till 2025. De omfattar cirka 360 aktörer, däribland privata företag och offentliga myndigheter från 26 medlemsstater samt från Norge, Island och Ukraina. Varje pilotprojekt är uppbyggt som ett konsortium som sammanför expertis från både den offentliga och den privata sektorn inom EU, med medfinansiering genom bidrag från Europeiska kommissionen. Pilotprojekten styrs av de tekniska specifikationer som utvecklats av eIDAS-expertgruppen.²⁰ I det följande redovisas kortfattat de fyra projektens ändamål och de länder som ingår i respektive konsortium.²¹

Potential-konsortiet omfattar fler än 140 offentliga och privata aktörer från 19 medlemsstater och Ukraina. I pilotprojektet testas användningsfallen mobila körkort, öppnande av bankkonto, registrering av SIM-kort, kvalificerade elektroniska underskrifter, tillgång till e-tjänster från offentlig förvaltning och elektroniska recept. Projektet samordnas av Frankrike och Tyskland.²²

NOBID-konsortiet omfattar aktörer från sex EU/EES-länder som fokuserar på användningsfallet betalningar för inhemsk och gränsöverskridande användning. Norge leder arbetet men i konsortiet ingår även Danmark, Lettland, Tyskland, Italien och Island.²³

EWC-konsortiet omfattar över 15 offentliga förvaltningar och 40 privata enheter från 18 medlemsstater och Ukraina. I pilotprojektet testas användningsfallen resor, betalningar och organisatorisk digital identitet. Samordnare för konsortiet är Sverige genom Bolagsverket.²⁴

DC4EU-konsortiet omfattar 99 institutioner från 25 länder med stöd av offentliga och privata organisationer, enheter och myndigheter. I pilotprojektet testas användningsfallen fri rörlighet med socialförsäkringsdokument som det europeiska hälso- och sjukvårdskortet

²⁰ <https://digital-strategy.ec.europa.eu/sv/policies/eudi-wallet-implementation> (hämtad 2025-05-19).

²¹ <https://digital-strategy.ec.europa.eu/sv/news/eu-digital-identity-4-projects-launched-test-eudi-wallet> (hämtad 2024-05-19).

²² <https://www.digital-identity-wallet.eu/> (hämtad 2024-05-20).

²³ <https://www.nobidconsortium.com/about/> (hämtad 2024-05-20).

²⁴ <https://eudiwalletconsortium.org/> (hämtad 2024-05-20).

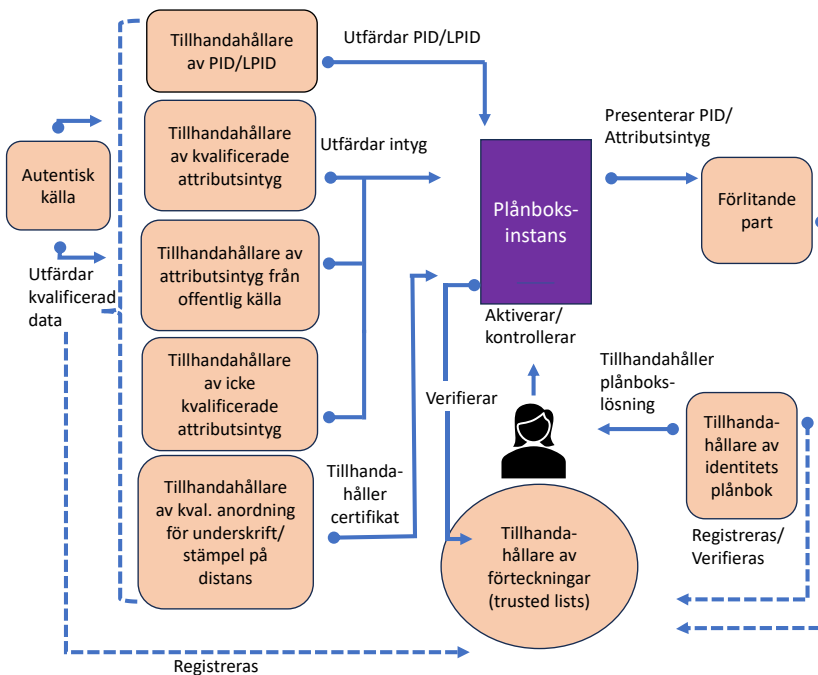
och utbildnings eller andra professionella kvalifikationer. Från Sverige deltar bl.a. Vetenskapsrådet/Sunet. Spanien är koordinator i arbetet.²⁵

4.7.4 Aktörer som är involverade i den europeiska digitala identitetsplånboken

I detta avsnitt presenteras de aktörer som är involverade i den europeiska digitala identitetsplånboken. Beskrivningen av aktörerna är hämtad från den ovan beskrivna arkitektur- och referensramen, ARF:en.²⁶

Figur 4.4 nedan visar en översikt över hur några centrala aktörer förhåller sig till varandra.

Figur 4.4 Översikt över vissa involverade aktörer



Källa: ARF version 1.4.0.

²⁵ <https://www.dc4eu.eu/project/> (hämtad 2024-05-20).

²⁶ The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework – Architecture and Reference Framework, version 1.4.0.

Användare av europeiska digitala identitetsplånböcker

Användare av europeiska digitala identitetsplånböcker använder sin plånboksinstans för att ta emot, lagra och visa upp uppgifter för personidentifiering (PID, dvs. den engelska akronymen för ”personal identification data”), kvalificerade elektroniska attributsintyg, offentligt utfärdade elektroniska attributsintyg eller attributsintyg om sig själva, inklusive sådana som bevisar identiteten. Användaren kan också skapa kvalificerade elektroniska underskrifter och stämplat samt använda identitetsplånboken för att interagera med andra identitetsplånböcker.

Tillhandahållare av europeiska digitala identitetsplånböcker

Tillhandahållare av europeiska digitala identitetsplånböcker kan vara en medlemsstat eller en privat aktör som uppdras av eller erkänns av medlemsstaten för att tillhandahålla identitetsplånböcker. Det är upp till respektive medlemsstat att bestämma villkoren för de privata aktörerna (se våra förslag i avsnitt 6.3.1 och 6.3.2).

Tillhandahållaren av identitetsplånboken ska tillse att användaren erbjuds en identitetsplånbokinstant som ger denne full kontroll över sin PID, sina elektroniska attributsintyg och alla andra personuppgifter som finns i identitetsplånboken.

Tillhandahållare av PID

Tillhandahållare av PID är betrodda aktörer som är ansvariga för att i) verifiera identiteten för plånboksanvändare i överensstämmelse med kraven enligt tillitsnivå hög, ii) utfärda PID till identitetsplånböcker och iii) tillgängliggöra information för förlitande parter för att möjliggöra validering av PID. Tillhandahållare av PID kan enligt förordningen exempelvis vara den aktör som utfärdar offentliga identitetshandlingar, elektroniska identitetshandlingar eller tillhandahållare av europeiska digitala identitetsplånböcker. Det är upp till varje medlemsstat att bestämma villkoren för ifrågakvarande tjänster (se våra förslag i avsnitt 6.3.3).

Tillhandahållare av förteckningar för validering

I ARF:en anges ”trusted list providers” som en aktör. För att särskilja dessa aktörer och förteckningar från den tillitsförteckning med uppgifter om kvalificerade tillhandahållare av betrodda tjänster och de kvalificerade betrodda tjänster som dessa tillhandahåller, som i Sverige sköts av PTS, kommer vi att benämna dessa aktörer som tillhandahållare av förteckningar för validering (se mer om tillitsförteckningen i avsnitt 4.10.7).

Den reviderade eIDAS-förordningen ställer krav på att vissa delar av identitetsplånbokens ekosystem ska kunna valideras. Detta är en central funktion i den tillitsmodell som presenteras i ARF:en.²⁷ Inom ramen för identitetsplånbokens ekosystem finns behov av förteckningar för validering från åtminstone följande tillhandahållare:

- tillhandahållare av identitetsplånböcker,
- tillhandahållare av PID,
- tillhandahållare av kvalificerade attributsintyg och
- tillhandahållare av attributsintyg från autentisk källa.

I ARF:en nämns, utöver de ovan listade förteckningarna, en förteckning över certifikatutfärdare²⁸ som utfärdar certifikat till tillhandahållare av PID, tillhandahållare av register över förlitande parter, tillhandahållare av kvalificerade attributsintyg och tillhandahållare av attributsintyg från autentisk källa. Användningen av termen certifikat i ARF:en och beskrivningen av tillitsmodellen leder till att en naturlig koppling kan göras till den ovan nämnda tillitsförteckningen. Enligt ARF:en ska detta dock inte ses som att det utgör en presumtion för att en viss teknisk lösning ska användas. Beroende på implementeringen är även andra tekniska lösningar möjliga och ska inte vara styrande gällande tillitsmodellen.²⁹ Tillitsmodellen beskrivs i ARF:en som konceptuell och att implementeringen kan ske på olika sätt, exempelvis att alla förteckningar kan samlas i en gemensam förteckning.³⁰

²⁷ The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework – Architecture and Reference Framework, version 1.4.0, avsnitt 6.

²⁸ A.a., avsnitt 3.4.

²⁹ A.a., avsnitt 6.1.1.

³⁰ Ibid.

Tillhandahållare av kvalificerade elektroniska attributsintyg

Kvalificerade elektroniska attributsintyg tillhandahålls av kvalificerade tillhandahållare av betrodda tjänster. Dessa träffas av kraven på kvalificerade tillhandahållare och tjänster i förordningen men dessa tjänster behöver även omfattas av vissa specifika krav som möjliggör användning av attributen i identitetsplånboken. Det handlar om att attesterings-tjänsten och identitetsplånboken behöver kunna identifiera sig för varandra och det kan behövas gränssnitt mot autentiska källor. Tillhandahållare av elektroniska attributsintyg behöver vidare ha information om var validering av attribut kan ske men det behöver finnas mekanismer som samtidigt inte visar i vilka e-tjänster attesteringarna används.

Tillhandahållare av attributsintyg från ett offentligt organs autentiska källa

Attributsintyg från ett offentlig organs autentiska källa utfärdas av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa. De krav som autentiska källor ställer för utfärdande och drift av ifrågavarande attributsintyg är avsedda att säkerställa att förlitande parter kan uppfatta den som kvalificerade attributsintyg.

Tillhandahållare av icke-kvalificerade attributsintyg

Elektroniska attributsintyg kan tillhandahållas av alla tillhandahållare av betrodda tjänster. De omfattas av händelsestyrd tillsyn under förordningen men de flesta sådana tillhandahållare regleras via avtal gällande regler, kommersiella villkor, erkännande och användningsområden. Dessa områden kan vara sådana som t.ex. körkort, digitala betalningar, utbildningsbevis. För att sådana icke-kvalificerade attesterade attribut ska kunna användas med den digitala identitetsplånboken behöver tillhandahållarna av sådana attribut, tekniskt följa de gränssnittskrav som identitetsplånboken uppställer.

Utfärdare av kvalificerade och icke-kvalificerade certifikat för elektroniska underskrifter och stämplat

Identitetsplånboken ska enligt förordningen kunna användas för att skapa kvalificerade elektroniska underskrifter eller stämplat. Det kan ske genom att identitetsplånboken certifieras som en anordning för framställning av kvalificerade elektroniska underskrifter eller stämplat. Det andra alternativet är att identitetsplånboken möjliggör säker läsning av en annan lokal anordning för underskrifter som t.ex. ett kort via NFC eller för autentisering till en distansunderskriftslösning där tillhandahållaren eller någon annan tillhandahåller anordningen för skapande av kvalificerade elektroniska underskrifter.

Autentiska källor

Autentiska källor är offentliga eller privata register som innehåller attribut om juridiska eller fysiska personer och som ses som grundkällan för dessa attribut. Enligt den reviderade eIDAS-förordningens bilaga VI ska ansvariga för autentiska källor ha ett gränssnitt till kvalificerade tillhandahållare av elektroniska attributsintyg som möjliggör att riktigheten hos ett attribut kan verifieras direkt hos den autentiska källan eller via ombud för den autentiska källan.

Förlitande parter

Förlitande parter är fysiska eller juridiska personer som förlitar sig på elektronisk identifiering eller betrodda tjänster. I sammanhanget med identitetsplånboken är förlitande parter de som efterfrågar attribut från PID eller andra attesteringar från innehavaren av identitetsplånboken. För att en förlitande part ska få förlita sig på plånboken ska den förlitande parten informera medlemslandet där denne är etablerad. Medlemslandet ska då föra upp den förlitande parten i ett register. Förlitande parter behöver ha ett gränssnitt mot plånboken för att kunna efterfråga attribut och för autentisering av den förlitande parten och plånboken. Förlitande parter är också skyldiga att kontrollera PID och andra attributs giltighet vid användning.

Organ för bedömning av överensstämmelse

Den digitala identitetsplånboken ska vara certifierad av ett ackrediterat organ för bedömning av överensstämmelse. Organet ska pekats ut av medlemsstaten. Kvalificerade tillhandahållare av betrodda tjänster och dess kvalificerade betrodda tjänster ska återkommande kontrolleras av ett organ för bedömning av överensstämmelse. Organet för bedömning av överensstämmelse ska ackrediteras av ett nationellt ackrediteringsorgan. Standarder och certifieringsordningar kommer att tas fram inom ramen för arbetet med den s.k. verktygslådan och kommer sedermera finnas i genomförandeakter.

Tillsynsorgan

Tillsynsorganens roll är att granska och säkerställa funktionaliteten hos tillhandahållare av europeiska digitala identitetsplånböcker och andra relevanta aktörer. Tillsynsorganen ska utses av medlemsstaterna och anmälas till kommissionen av medlemsstaten, se våra förslag rörande tillsyn i avsnitt 6.6.

4.7.5 Identitetsplånbokslösningen, identitetsplånboksinstansen och PID

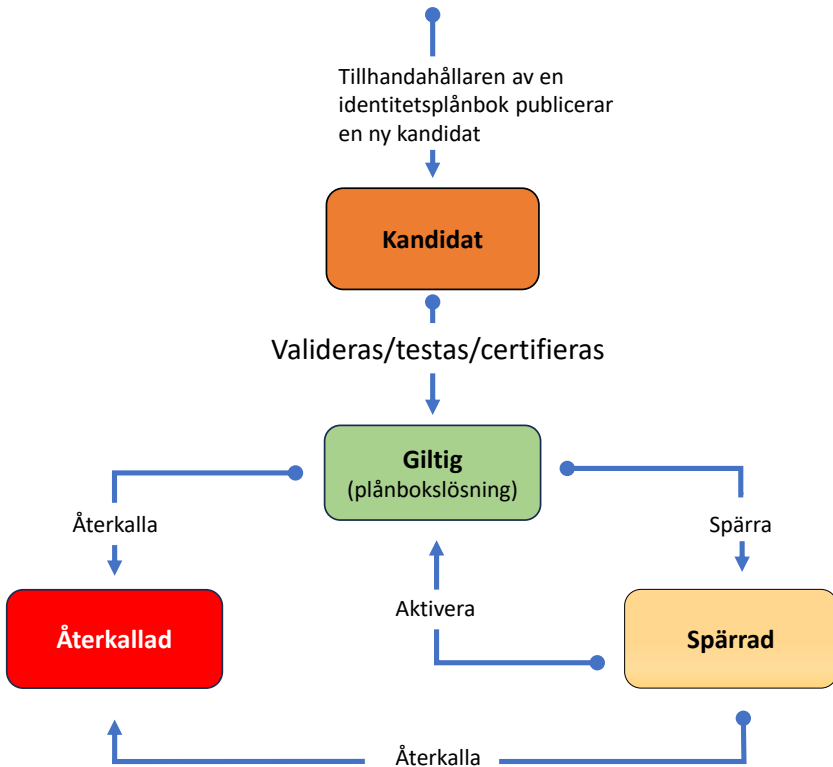
I detta avsnitt redovisas hur en identitetsplånbokslösning, en identitetsplånboksinstans och PID förhåller sig till varandra.

Identitetsplånbokslösningen

En identitetsplånbokslösning befinner sig, under sin livscykel, i olika stadier i enlighet med vad som framgår av artikel 5d. Aktuellt stadie påverkar samtliga identitetsplånboksinstanser som tillhandahållits inom ramen för lösningen.

Figur 4.5 nedan visar identitetsplånbokslösningens olika faser.

Figur 4.5 Identitetsplånbokslösningens olika faser



Källa: ARF 1.4.0.

Kandidatstadiet är det första stadiet för identitetsplånbokslösningen. Lösningen är då fullt implementerad och tillhandahållaren kan ansöka om att lösningen ska bli certifierad.

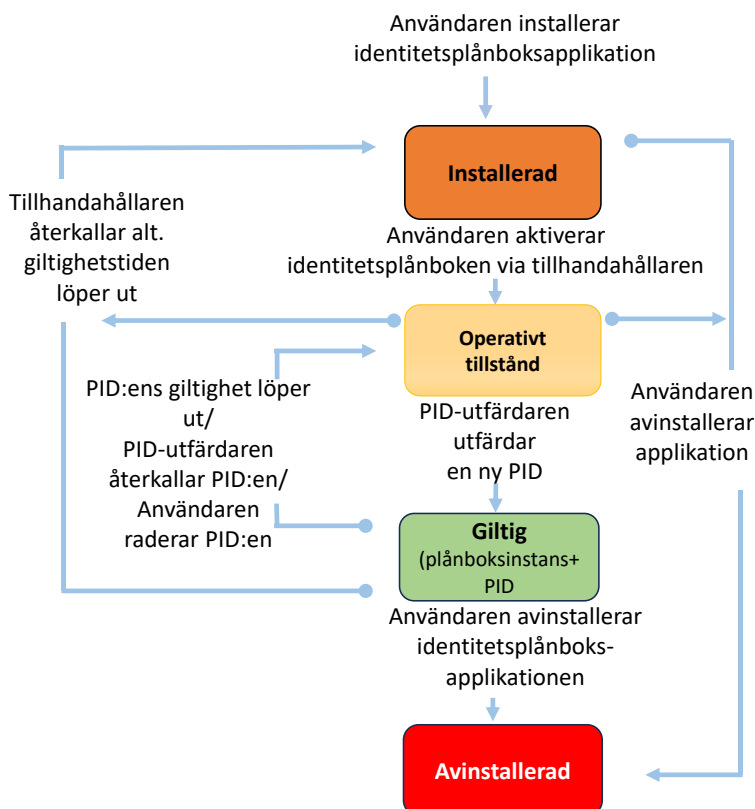
Om identitetsplånbokslösningen uppfyller relevanta krav kan medlemsstaten besluta att identitetsplånboksinstanter får tillhandahållas. Identitetsplånbokslösningen är då i stadiet ”giltig”.

I enlighet med vad som följer av artikel 5e kan en medlemsstat tillfälligt spärra en viss identitetsplånbokslösning, besluta att upphäva spärren (dvs. aktivera lösningen igen) alternativt återkalla den helt (se våra förslag i avsnitt 6.6.3).

Identitetsplånboksinstansen

En identitetsplånboksinstans livscykel inleds när användaren installerar en applikation från en giltig identitetsplånbokslösning till sin användarenhet. Instansens status övergår då till installerad. Figur 4.6 nedan illustrerar identitetsplånboksinstansens olika stadier.

Figur 4.6 Identitetsplånboksinstansens olika faser



Källa: ARF Version 1.4.0.

Efter att användaren, via tillhandahållaren av vald identitetsplånbokslösning, aktiverat plånboksinstansen är den i operativt tillstånd. I det operativa tillståndet är det användaren som hanterar plånboksinstansen, men det kan involvera att tillhandahållaren uppdaterar instansen, återkallar instansen (även på begäran av användaren) eller att användaren

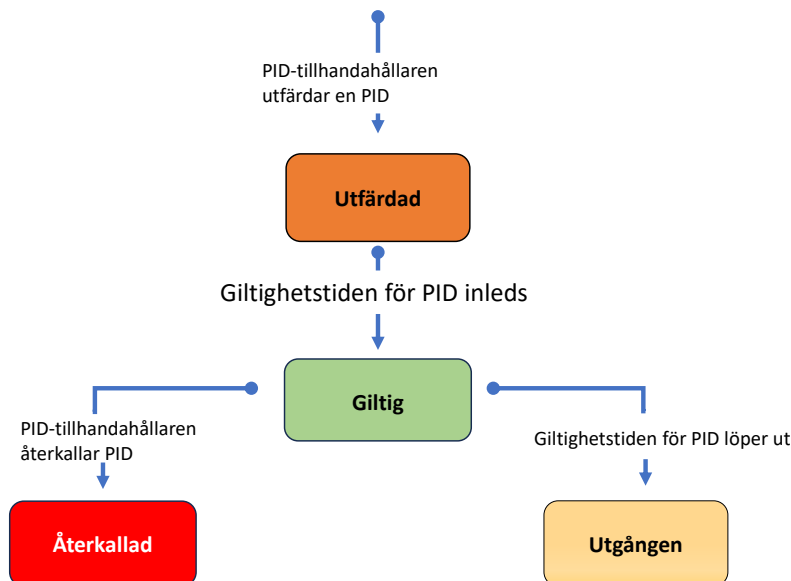
avinstallerar plånboksinstansen. I det operativa stadiet kan användaren begära utfärdande av PID och valfria attributsintyg.

När en identitetsplånboksinstans innehåller en giltig PID är den att betrakta som giltig. Detta stadie kan inte uppnås utan att en PID begärs. I stadiet giltig kan användaren använda sin identitetsplånboksinstans för att visa upp PID-attribut. Om giltigheten av PID löper ut, eller om PID återkallas, blir identitetsplånboksinstansen inte automatiskt obrukbar, men dess stadie återgår till operativt. Detta kan i sin tur påverka giltigheten av och möjligheten att använda olika attributsintyg.

Personidentifieringsuppgifter (PID)

Inom ramen för den europeiska digitala identitetsplånboken inleds livscykeln för PID när den utfärdas till en identitetsplånboksinstans. När giltighetstiden för PID inleds övergår den från att vara utfärdad till att vara giltig. Giltighetstiden kan avslutas genom att den löper ut eller genom att den återkallas av PID-tillhandahållaren. Därefter kan PID aldrig återgå till att vara giltig igen utan en ny PID måste, om förutsättningar för det finns, utfärdas. Figur 4.7 nedan illustrerar olika faser för PID.

Figur 4.7 PID:ens olika faser



Källa: ARF 1.4.0.

4.8 Befintliga betrodda tjänster

4.8.1 Elektroniska underskrifter

I artikel 3.10 i eIDAS-förordningen definieras en elektronisk underskrift som uppgifter i elektronisk form som är fogade till eller logiskt knutna till andra uppgifter i elektronisk form och som används av undertecknaren för att skriva under. Detta är den grundläggande definitionen av elektronisk underskrift och det är således en elektronisk underskrift som varken är avancerad eller kvalificerad. En sådan underskrift skulle t.ex. kunna vara att skriva sitt namn under ett e-postmeddelande.

Avancerade elektroniska underskrifter

Utöver den grundläggande definitionen av elektroniska underskrifter definierar eIDAS-förordningen två andra typer av underskrifter: avancerade (artikel 3.11) och kvalificerade (artikel 3.12). På dessa ställs krav som går utöver grunddefinitionen. En avancerad elektronisk underskrift ska uppfylla de krav som uppställs i artikel 26. Detta innebär att

- a) Den ska vara unikt knuten till undertecknaren.
- b) Undertecknaren ska kunna identifieras genom den.
- c) Den ska vara skapad på grundval av uppgifter för skapande av elektroniska underskrifter som undertecknaren med hög grad av tillförlitlighet kan använda uteslutande under sin egen kontroll.
- d) Den ska vara kopplad till de uppgifter som den används för att underteckna på ett sådant sätt att alla efterföljande ändringar av uppgifterna kan upptäckas.

Ytterligare krav än de som framgår ovan ställer eIDAS-förordningen inte upp avseende avancerade elektroniska underskrifter. Förordningen föreskriver inte heller hur det går att leva upp till dessa krav tekniskt.

Kommissionen ska enligt den reviderade eIDAS-förordningens artikel 26.2 senast den 21 maj 2026 bedöma behovet av en genomförandeakt som pekar ut standarder, specifikationer eller förfaranden för avancerade elektroniska underskrifter. En sådan genomförandeakt skulle om en tillhandahållare följer den, ge en presumtion om att de

uppfyller kraven för avancerade elektroniska underskrifter. Det finns en befintlig genomförandeakt enligt artikel 27.5 i eIDAS-förordningen som pekar ut ett antal tekniska specifikationer avseende elektroniska underskrifter.³¹ Dessa är dock de format som medlemsstaterna ska erkänna avseende avancerade elektroniska underskrifter som är i enlighet med dessa specifikationer. Genomförandebeslutet ska dock inte tolkas som att det uteslutande är dessa tekniska specifikationer som kan användas för att en avancerad elektronisk underskrift ska uppfylla kraven i artikel 26.

Kvalificerade elektroniska underskrifter

För att en elektronisk underskrift ska vara kvalificerad ställs ytterligare krav. En sådan underskrift ska uppfylla samma krav som en avancerad elektronisk underskrift och därtill skapas med en kvalificerad anordning för underskriftsframställning samt baseras på ett kvalificerat certifikat för elektroniska underskrifter. De detaljerade kraven återfinns delvis i bilaga I till eIDAS-förordningen, delvis i bilaga I till den reviderade eIDAS-förordningen. Där framgår att sådana certifikat ska innehålla bl.a. uppgifter om den kvalificerade tillhandahållare av betrodda tjänster som utfärdar certifikaten, undertecknarens namn eller en pseudonym, uppgifter om när certifikatet börjar respektive upphör att gälla samt certifikatets identifieringskod. Koden måste vara unik för den aktuella kvalificerade tillhandahållaren av betrodda tjänster.

Kommissionen ska med stöd av artikel 28.6 senast den 21 maj 2025 ta fram genomförandeakter som upprättar förteckning över referensstandarder och vid behov specifikationer och förfaranden för kvalificerat certifikat för elektroniska underskrifter. Vidare finns det i artikel 24.1 a krav på kvalificerade tillhandahållare att, när de utfärdar ett kvalificerat certifikat för en betrodd tjänst, på lämpligt sätt kontrollera identiteten och i förekommande fall eventuella särskilda attribut för den fysiska eller juridiska person till vilken det kvalificerade certifikatet utfärdas. Informationen kan kontrolleras genom fysisk

³¹ Kommissionens genomförandebeslut (EU) 2015/1506 av den 8 september 2015 om fastställande av specifikationer rörande format för avancerade elektroniska underskrifter och avancerade elektroniska stämplat i enlighet med artiklarna 27.5 och 37.5 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden.

närvaro av den fysiska personen eller fysisk närvaro av en behörig företrädare för en juridisk person. Kontroll kan också under vissa förutsättningar ske på distans med hjälp av medel för elektronisk identifiering eller genom ett certifikat för en kvalificerad elektronisk underskrift eller stämpel som har utfärdats genom fysisk närvaro eller på distans. Informationen kan även kontrolleras med hjälp av andra identifieringsmetoder som erbjuder garantier som är likvärdiga med fysisk närvaro. EU-kommissionen ska enligt artikel 24.1 c senast den 21 maj 2024 genom genomförandeakter, upprätta en förteckning över referensstandarder och vid behov fastställa specifikationer och förfaranden för kontroll av identitet och attribut.

Anordningar för underskriftframställning

En anordning för underskriftframställning definieras i artikel 3.22 som en konfigurerad programvara eller maskinvara som används för att skapa en elektronisk underskrift. Anordningen är en skyddad miljö för lagring och användning av privata nycklar som smarta kort eller s.k. HSM-moduler.³² Förordningen innehåller endast krav på kvalificerade sådana anordningar. Dessa ska uppfylla kraven i bilaga II till eIDAS-förordningen och i bilaga II i den reviderade eIDAS-förordningen. I bilagan finns ett flertal krav, bl.a. att kvalificerade anordningar för skapande av elektroniska underskrifter genom lämpliga tekniker och förfaranden ska säkerställa att de uppgifter för skapande av elektroniska underskrifter som används för att skapa elektroniska underskrifter i praktiken endast kan förekomma en gång och att den elektroniska underskriften på ett tillförlitligt sätt är skyddad mot förfalskning med den teknik som för närvarande finns tillgänglig. Anordningar för skapande av kvalificerade elektroniska underskrifter och stämplat ska certifieras av offentliga eller privata organ som utsetts av medlemsstaterna. Kommissionen har i ett genomförandebeslut fastställt de standarder för säkerhetsbedömning av informationsteknikprodukter som gäller för certifiering av kvalificerade anordningar för skapande av

³² Hardware Security Module

elektroniska underskrifter eller kvalificerade anordningar för skapande av elektroniska stämplat.³³

Validering av avancerade elektroniska underskrifter baserade på kvalificerade certifikat och av kvalificerade elektroniska underskrifter

Som framgår ovan innehåller den reviderade eIDAS-förordningen även krav som avser validering av avancerade elektroniska underskrifter baserade på kvalificerade certifikat. Enligt artikel 32a ska en avancerad elektronisk underskrifts giltighet bekräftas om processen för validering enligt nedan följs:

- a) Certifikatet som användes för att skapa underskriften vid tidpunkten för undertecknandet var ett kvalificerat certifikat för elektroniska underskrifter som överensstämmer med förordningens bilaga I.
- b) Det kvalificerade certifikatet var utfärdat av en kvalificerad tillhandahållare av betrodda tjänster och var giltigt vid tidpunkten för undertecknandet.
- c) Valideringsuppgifterna för underskriften överensstämmer med de uppgifter som lämnats till den förlitande parten.
- d) Certifikatets unika uppsättning uppgifter som avser undertecknaren har tillhandahållits den förlitande parten på rätt sätt.
- e) Användningen av en eventuell pseudonym har tydligt angetts för den förlitande parten om en pseudonym användes vid tidpunkten för undertecknandet.
- f) Integriteten hos de undertecknade uppgifterna inte har äventyrats.
- g) Kraven i artikel 26 var uppfyllda vid tidpunkten för undertecknandet.

³³ Kommissionens genomförandebeslut (EU) 2016/650 av den 25 april 2016 om fastställande av standarder för säkerhetsbedömning av kvalificerade anordningar för skapande av elektroniska underskrifter och stämplat enligt artiklarna 30.3 och 39.2 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden.

Av artikel 32a.2 framgår att det system som används för att validera den kvalificerade elektroniska underskriften ska ge den förlitande parten det korrekta resultatet av valideringsförfarandet och göra det möjligt för den förlitande parten att upptäcka eventuella problem som är relevanta för säkerheten. Senast den 21 maj 2025 ska kommissionen med stöd av artikel 32a.3 genom genomförandeakter fastställa förteckning med referensstandarder och vid behov fastställa specifikationer och förfaranden för validering av avancerade elektroniska underskrifter baserade på kvalificerade certifikat.

Krav avseende kvalificerade valideringstjänster för kvalificerade elektroniska underskrifter finns i artikel 32. Även för kvalificerade valideringstjänster ska kommissionen, med stöd av artikel 32.3, senast den 21 maj 2025 anta genomförandeakter med förteckning över referensstandarder och vid behov fastställa specifikationer och förfaranden för kvalificerade valideringstjänster.

Kvalificerade bevarandetjänster av kvalificerade elektroniska underskrifter

I artikel 34 ställs krav på kvalificerade tjänster för bevarande av kvalificerade elektroniska underskrifter. Sådana tjänster får endast tillhandahållas av kvalificerade tillhandahållare av betrodda tjänster som använder förfaranden och tekniker som gör det möjligt att förlänga den kvalificerade elektroniska underskriftens tillförlitlighet utöver perioden för teknisk giltighet. Utöver det innehåller förordningen inga bestämmelser om bevarande, utöver att bevarande av elektroniska underskrifter, stämplat eller certifikat med anknytning till dessa tjänster definieras som en betrodd tjänst (artikel 3.16). Kommissionen ska enligt artikel 34.2 senast den 21 maj 2025 genom genomförandeakter, upprätta en förteckning över referensstandarder och vid behov fastställa specifikation och förfaranden för kvalificerade tjänster för bevarande av kvalificerade elektroniska underskrifter.

4.8.2 Elektroniska stämplat

Sett till både den bakomliggande tekniken och utformningen av de bestämmelser som reglerar elektroniska stämplat och elektroniska underskrifter finns det stora likheter mellan dessa två typer av utställar-

verifikationer. Den avgörande skillnaden utgörs av vem som skapar en elektronisk underskrift respektive stämpel. Elektroniska stämplat skapas av juridiska personer (artikel 36), till skillnad från elektroniska underskrifter som skapas av fysiska personer (artikel 26). En elektronisk stämpel definieras i förordningen som uppgifter i elektronisk form som är fogade eller logiskt knutna till andra uppgifter i elektronisk form för att säkerställa den senares ursprung och integritet (artikel 3.24). Definitionen är snarlik den för elektroniska underskrifter men det finns alltså inte någon undertecknare när det gäller stämplat. I likhet med vad som gäller för elektroniska underskrifter finns det i förordningen olika nivåer av elektroniska stämplat. Utöver grunddefinitionen finns avancerade elektroniska stämplat samt kvalificerade elektroniska stämplat. Systematiken när det gäller kraven är dessutom densamma. En avancerad elektronisk stämpel ska leva upp till kraven i artikel 36. Detta innebär att

- a) Den ska vara knuten uteslutande till skaparen av stämplat.
- b) Skaparen av stämplat ska kunna identifieras genom det.
- c) Det ska vara skapat på grundval av uppgifter för skapande av elektroniska stämplat som stämplatns skapare med hög grad av tillförlitlighet under sin kontroll kan använda för skapande av elektroniska stämplat.
- d) Den ska vara kopplad till de uppgifter den avser på ett sådant sätt att alla efterföljande ändringar av uppgifterna kan upptäckas.

En kvalificerad elektronisk stämpel ska enligt artikel 3.27, i likhet med vad som gäller för underskrifter, leva upp till kraven på en avancerad elektronisk stämpel samt skapas med hjälp av en kvalificerad anordning för skapande av elektroniska stämplat och som är baserat på ett kvalificerat certifikat för elektroniska stämplat. Kraven för stämplat är i stora delar desamma som för elektroniska underskrifter, med den skillnaden att kraven för stämplaterna i relevanta delar hänvisar till skaparen av stämplat i stället för undertecknaren. Ett illustrerande exempel är kraven på kvalificerat certifikat för elektroniska stämplat som fastställs i dels bilaga III i eIDAS-förordningen, dels bilaga III i den reviderade eIDAS-förordningen. Den enda skillnaden gentemot underskrifter är att det för stämplat finns krav på att information om skaparen av stämplat ska finnas (namn och i förekommande fall registrerings-

nummer) medan det för underskrifter ska finnas information om undertecknaren.

Även de betrodda tjänsterna validering och bevarande av elektroniska stämplat regleras i förordningen och de har då exakt samma ordalydelse som bestämmelserna för validering av elektroniska underskrifter och bevarande av elektroniska underskrifter. Motsvarande delegation till EU-kommissionen att ta fram genomförandeakter finns med samma ordalydelse, t.ex. för avancerade elektroniska stämplat enligt artikel 36.2 som för avancerade elektroniska underskrifter enligt artikel 26.2.

4.8.3 Elektronisk tidsstämpling

I förordningen definieras elektronisk tidsstämpling i artikel 3.33 som uppgifter i elektronisk form som binder andra uppgifter i elektronisk form till en viss tidpunkt och därmed utgör bevis för att de senare uppgifterna existerade vid den tidpunkten. Betrodda tjänster som avser tidsstämpling kan vara kvalificerade eller icke-kvalificerade. För icke-kvalificerade tjänster innehåller förordningen inga krav utöver definitionen. Kvalificerad elektronisk tidsstämpling ska däremot enligt artikel 42 uppfylla följande bestämmelser:

- a) Den ska binda datumet och tiden till uppgifter så att möjligheten att uppgifterna ändras utan att det går att upptäcka rimligtvis kan uteslutas.
- b) Den ska vara grundad på en korrekt tidskälla som är kopplad till samordnad universaltid.
- c) Den ska vara undertecknad med hjälp av en avancerad elektronisk underskrift eller förseglad med en avancerad elektronisk stämpel från den kvalificerade tillhandahållaren av betrodda tjänster eller genom en likvärdig metod.

En kvalificerad elektronisk tidsstämpling ska enligt artikel 41 i eIDAS-förordningen omfattas av en presumtion om korrekthet hos det datum och den tid som den anger och integritet hos de uppgifter som datumet och tiden är kopplade till. Kommissionen ska enligt artikel 42.2 senast den 21 maj 2025 genom genomförandeakter upprätta en förteckning över referensstandarder och vid behov fastställa specifikationer och

förfaranden för bindning av datum och tidpunkt till uppgifter och fastställande av korrektheten för tidskällor avseende kvalificerade elektroniska tidsstämplingar.

4.8.4 Certifikat för autentisering av webbplatser

Ett certifikat för autentisering av webbplatser definieras i artikel 3.38 i den reviderade eIDAS-förordningen som ett elektroniskt intyg som gör det möjligt att autentisera en webbplats och kopplar webbplatsen till den fysiska eller juridiska person som certifikatet utfärdats för. Även för autentisering av webbplatser kan certifikaten, och i förlängningen tjänsterna, vara kvalificerade eller icke-kvalificerade. Inga särskilda bestämmelser, utöver definitionen, finns för de icke-kvalificerade certifikaten. Krav som kvalificerat certifikat för autentisering av webbplatser ska uppfylla finns emellertid. Dels ska ett kvalificerat certifikat utfärdas av en kvalificerad tillhandahållare av betrodda tjänster, dels uppfylla kraven i bilaga IV till eIDAS-förordningen och den reviderade eIDAS-förordningen (artikel 45 och artikel 24.1 a). Kommissionen ska senast den 21 maj 2025 med stöd av artikel 45.2 genom genomförandeakter upprätta en förteckning över referensstandarder och vid behov fastställa specifikationer och förfaranden för kvalificerat certifikat för autentisering av webbplatser. Förordningen ställer även i artikel 45.1 a krav på att vissa uppgifter som ytterligare attribut från kvalificerat certifikat för autentisering av webbplatser av webbläsarna, på ett användarvänligt sätt visas för besökarna på en webbplats som använder ett kvalificerat certifikat för autentisering av webbplatser.

4.8.5 Elektronisk tjänst för rekommenderad leverans

Elektroniska tjänster för rekommenderade leveranser gör, enligt definitionen i artikel 3.36 i eIDAS-förordningen, det möjligt att överföra uppgifter mellan tredje män på elektronisk väg och tillhandahåller bevis avseende de överförda uppgifternas hantering, inklusive bevis för uppgifternas sändning och mottagande, och som skyddar överförda uppgifter mot risken för förlust, stöld, skada eller otillåtna ändringar. Ytterligare vägledning om hur termen ska tolkas och tillämpas ger inte förordningen. Däremot framgår av skäl 66 i den ursprungliga eIDAS-

förordningen att det är av avgörande betydelse att det föreskrivs en rättslig ram för att främja gränsöverskridande erkännande mellan befintliga nationella rättssystem för elektroniska tjänster för rekommenderade leveranser. Vidare framgår av samma skältext att den ramen skulle kunna öppna nya marknadsmöjligheter för unionens tillhandahållare av betrodda tjänster att erbjuda nya paneuropeiska tjänster för elektroniska tjänster för rekommenderade leveranser.

Elektroniska tjänster för rekommenderade leveranser kan vara kvalificerade eller icke-kvalificerade. Bestämmelser utöver definitionen för icke-kvalificerade tjänster saknas i förordningen. De krav som ställs på kvalificerade elektroniska tjänster för rekommenderade leveranser är bl.a. att de ska tillhandahållas av en eller flera kvalificerade tillhandahållare av betrodda tjänster, att de med hög grad av tillförlitlighet ska säkerställa avsändarens identitet och att de ska säkerställa adressatens identitet innan uppgifterna levereras (artikel 44.1).

Om uppgifterna överförs mellan två eller flera kvalificerade tillhandahållare av betrodda tjänster ska kraven gälla för alla involverade kvalificerade tillhandahållare av betrodda tjänster. Av artikel 44.2 a framgår att kvalificerade tillhandahållare av kvalificerade tjänster för elektronisk rekommenderad leverans får komma överens om interoperabilitet mellan de tjänster som de tillhandahåller. Ett ramverk för interoperabilitet ska uppfylla kraven i punkt 1 och efterlevnaden ska kontrolleras av ett organ för bedömning av överensstämmelse. Kommissionen får ta fram genomförandeakter som pekar ut standarder eller specifikationer och procedurer för interoperabilitet enligt ovanstående stycke.

Kommissionen ska även enligt artikel 44.2 senast den 21 maj 2025 genom genomförandeakter upprätta en förteckning över referensstandarder och vid behov fastställa specifikationer och förfaranden för processer för att sända och ta emot uppgifter avseende kvalificerade elektroniska tjänster för rekommenderade leveranser. Kommissionen får vidare enligt artikel 44.2 b genom genomförandeakter upprätta en förteckning över referensstandarder och vid behov fastställa specifikationer och förfaranden för interoperabilitetsramverk på området.

4.9 Nya betrodda tjänster

4.9.1 Kvalificerade tjänster för förvaltning av anordningar för skapande av elektroniska underskrifter på distans

Kvalificerade tjänster för förvaltning av anordningar för skapande av elektroniska underskrifter på distans ska enligt definitionen i artikel 3.23a omfattas av kraven i artikel 29a och bestå av att en kvalificerad tillhandahållare av betrodda tjänster genererar, förvaltar och kopierar den data som skapar den elektroniska underskriften för undertecknarens räkning. En anordning för skapande av elektroniska underskrifter är enligt definitionen i artikel 3.22 i eIDAS-förordningen en konfigurerad programvara eller maskinvara som används för att skapa en elektronisk underskrift. Anordningen är en skyddad miljö för lagring och användning av privata nycklar.

Kraven på den som tillhandahåller en sådan tjänst finns i artikel 29a i den reviderade eIDAS-förordningen och av kraven framgår att det enbart är kvalificerade tillhandahållare av betrodda tjänster som får generera och hantera data för skapandet av elektroniska underskrifter åt undertecknaren. Data får säkerhetskopieras men ska då ha minst samma skydd som de lagrade nycklarna och antalet lagrade säkerhetskopior av nycklar ska inte överstiga det som krävs för kontinuitet i tjänsten. Vidare ska alla kraven som finns i samband med certifieringen av anordningen i enlighet med artikel 30 följas.

Kommissionen ska senast 12 månader efter den reviderade förordningen ikraftträdande ta den 21 maj 2025 genom genomförandeakter upprätta en förteckning över referensstandarder och vid behov specifikationer och förfaranden för att hantera tjänsten.

4.9.2 Elektroniska attributsintyg

Den betrodda tjänsten elektroniska attributsintyg kommer att användas tillsammans med den digitala identitetsplånboken. Identitetsplånboken är tänkt att, utöver en elektronisk identitet, kunna innehålla ett antal attribut om innehavaren. Av definitionen i artikel 3.43 i den reviderade eIDAS-förordningen framgår att ett attribut är en egenkap, en kvalitet, en rättighet eller ett tillstånd för en fysisk eller juridisk person eller ett föremål. Ett elektroniskt attributsintyg är enligt artikel 3.44, ett intyg i elektronisk form som möjliggör autentisering

av attribut. Vidare framgår av artikel 3.45 att ett kvalificerat elektroniskt attributsintyg är ett elektroniskt attributsintyg som utfärdats av en kvalificerad tillhandahållare av betrodda tjänster och uppfyller kraven i bilaga V. Elektroniska attributsintyg kan även enligt artikel 3.46 utfärdas av eller på uppdrag av offentligt organ som ansvarar för en autentisk källa som då ska uppfylla kraven i artikel 45f och bilaga VII. Enligt artikel 3.47 är en autentisk källa, samlingsplats eller system, som innehas under ansvar ett offentligt organ eller privat enhet, som innehåller och tillhandahåller attribut om en fysisk eller juridisk person eller ett föremål och som anses vara en primärkälla för den informationen eller erkänns som autentisk enligt unionsrätten eller nationell lagstiftning, inbegripet administrativa förfaranden.

Av kraven i artiklarna 45b–45h i den reviderade eIDAS-förordningen framgår bl.a. att den betrodda tjänsten elektroniska attributsintyg kan vara antingen en icke-kvalificerad tjänst, en kvalificerad sådan tjänst eller en tjänst som tillhandahålls av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa.

Alla tillhandahållare av elektroniska attributsintyg ska enligt artikel 45g tillhandahålla attributsintygen till de digitala identitetsplånböckerna på ett sätt som möjliggör för användare av den europeiska digitala identitetsplånboken att efterfråga, hämta, lagra och hantera attributsintygen oavsett i vilken medlemsstat som plånboken tillhandahålls. Elektroniska attributsintyg ska tillhandahållas till de identitetsplånböcker som tillhandahålls i enlighet med artikel 5a i den reviderade eIDAS-förordningen. Tillhandahållare av elektroniska attributsintyg får vidare enligt artikel 45h inte kombinera personuppgifter från den tjänsten med tillhandahållarens eventuella andra tjänster eller dess kommersiella partners tjänster. Vidare ska personuppgifter från intygstjänsten vara logiskt separerade från andra data som tillhandahållaren har.

Kvalificerade tjänster för elektroniska attributsintyg ska separera tjänsten mot andra tjänster som tillhandahållaren tillhandahåller. Enligt artikel 45b ska kvalificerade tillhandahållare av elektroniska attributsintyg förutsättas ha samma rättsverkan som attesteringar på papper. Elektroniska attributsintyg som tillhandahålls av ett offentligt organ som ansvarar för en autentisk källa ska vidare erkännas på samma sätt i alla medlemsländer.

Kraven på kvalificerade elektroniska attributsintyg återfinns i artikel 45d och i bilaga V och får inte omfattas av andra obligatoriska krav. Av bilaga V följer att kvalificerade attributsintyg ska innehålla

- En uppgift, åtminstone i en form som lämpar sig för automatiserad behandling, om att intyget har utfärdats som ett kvalificerat elektroniskt attributsintyg.
- En uppsättning uppgifter som otvetydigt avser den kvalificerade tillhandahållare av betrodda tjänster som utfärdar det kvalificerade elektroniska attributsintyget, inbegripet uppgift om åtminstone vilken medlemsstat tillhandahållaren är etablerad i, samt för en juridisk person: namn och, i tillämpliga fall, registreringsnummer i enlighet med vad som uppgetts i de officiella handlingarna, för en fysisk person: personens namn.
- En uppsättning uppgifter som otvetydigt avser den enhet som de intygade attributen hänvisar till; om en pseudonym används ska detta anges tydligt.
- Det intygade attributet eller de intygade attributen, inbegripet, i tillämpliga fall, de uppgifter som är nödvändiga för att fastställa omfattningen för dessa attribut.
- Detaljerade uppgifter om när intyget börjar respektive upphör att gälla.
- Intygets identitetskod, vilken måste vara unik för den kvalificerade tillhandahållaren av betrodda tjänster, och, i tillämpliga fall, uppgift om det intygssystem som attributsintyget omfattas av.
- Den kvalificerade elektroniska underskriften eller den kvalificerade elektroniska stämpeln för den utfärdande kvalificerade tillhandahållaren av betrodda tjänster.
- Uppgift om var det certifikat som stöder den kvalificerade elektroniska underskrift eller den kvalificerade elektroniska stämpel som avses i led g är tillgängligt kostnadsfritt.
- Information om det kvalificerade intygets giltighet, eller uppgift om var de tjänster som kan användas för att göra förfrågningar är lokaliserade.

Granskning av om en kvalificerad tillhandahållare av elektroniska attributsintyg uppfyller kraven görs genom att granska att kraven i bilaga V och de standarder, specifikationer och förfaranden enligt den genomförandeakt som kommissionen ska ta fram efterlevs. Kommis-

sionen ska senast den 21 november 2024 genom genomförandeakter upprätta en förteckning över referensstandarder och vid behov fastställa specifikationer och förfaranden för kvalificerade elektroniska attributsintyg. Vidare ska sådana attribut som spärrats inte kunna bli giltiga igen utan nya behöver då tillhandahållas.

Kraven på elektroniska attributsintyg som tillhandahålls av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa finns i artikel 45f och i bilaga VII. Kraven liknar det som gäller för kvalificerade tillhandahållare av tjänsten. Skillnaden är att medlemsstaten ska säkerställa att det offentliga organet som tillhandahåller tjänsten uppfyller motsvarande krav som kvalificerade tillhandahållare av betrodda tjänster. Vidare ska medlemsstaten notifiera de offentliga organ som ansvarar för en sådan tjänst till kommissionen. Notifieringen ska innehålla en bedömning av överensstämmelse från ett organ för bedömning av överensstämmelse som visar att kraven i artikel 45f och bilaga VII uppnås.

Kommissionen ska enligt artikel 45f.6 senast den 21 november 2024 genom genomförandeakter upprätta en förteckning över referensstandarder och vid behov specifikationer och förfaranden för tjänsten. Kommissionen ska vidare enligt artikel 45f.7 senast den 21 november 2024 genom en genomförandeakt upprätta en förteckning över referensstandarder och vid behov specifikationer och förfaranden avseende förfarandet för bedömning av överensstämmelse enligt ovan.

I artikel 45e i förordningen och i bilaga VI listas de attribut som medlemsstaterna ska vidta åtgärder för att göra det möjligt för kvalificerade tillhandahållare av elektroniska attributsintyg att kontrollera äktheten hos. Vidare ska det med elektroniska medel, och på begäran av användaren gå att kontrollera äktheten hos attributen via den relevanta autentiska källan på nationell nivå eller via särskilt utsedda mellanhänder som är erkända på nationell nivå i enlighet med nationell lagstiftning eller unionslagstiftning och i de fall då dessa attribut utgår från autentiska källor inom offentlig sektor. Detta gäller attributen:

- Adress
- Ålder
- Kön

- Civilstånd
- Familjesammansättning
- Nationalitet eller medborgarskap
- Utbildningskvalifikationer, titlar och licenser
- Yrkeskvalifikationer, titlar och licenser
- Befogenheter och uppdrag att företräda fysiska eller juridiska personer
- Offentliga tillstånd och licenser
- För juridiska personer, finansiella uppgifter och företagsuppgifter.

4.9.3 Elektroniska arkiveringstjänster

Elektronisk arkivering definieras i artikel 3.48 som en tjänst som säkerställer mottagande, lagring, hämtning och radering av elektroniska uppgifter och elektroniska dokument i syfte att säkerställa deras hållbarhet och läsbarhet samt att bevara deras integritet, konfidentialitet och ursprungsbevis under hela bevarandeperioden. Av artikel 45i framgår dess rättsliga verkan i punkt 1 och i punkt 2 den särskilda presumtion som kvalificerade elektroniska arkivtjänster omfattas av vad gäller integritet och ursprung under perioden av bevarandet hos den kvalificerade arkivtjänsten. Det finns inga specifika krav avseende icke-kvalificerade arkivtjänster i förordningen.

Kraven på kvalificerade tillhandahållare av kvalificerade elektroniska arkivtjänster finns i artikel 45j:

- Tjänsten tillhandahålls av en kvalificerad tillhandahållare.
- Tillhandahållaren ska använda förfaranden och teknik som kan säkerställa att elektroniska uppgifter och elektroniska dokument håller och är läsbara även efter den tekniska giltighetstiden och åtminstone under hela den rättsliga eller avtalsenliga bevarandeperioden, samtidigt som deras integritet och korrekta ursprung bibehålls.
- Tillhandahållaren ska säkerställa att dessa elektroniska uppgifter och elektroniska dokument bevaras på ett sådant sätt att de skyddas

mot förlust och ändring, med undantag för ändringar som rör deras medium eller elektroniska format.

- De ska göra det möjligt för behöriga förlitande parter att ta emot en rapport på ett automatiserat sätt som bekräftar att elektroniska uppgifter och elektroniska dokument som hämtats från ett kvalificerat elektroniskt arkiv omfattas av presumtionen om uppgifternas integritet från början av bevarandeperioden till tidpunkten för hämtningen.
- Den rapport som avses i första stycket led d ska tillhandahållas på ett tillförlitligt och effektivt sätt och ska vara försedd med den kvalificerade elektroniska underskriften eller den kvalificerade elektroniska stämpeln för tillhandahållaren av den kvalificerade elektroniska arkiveringstjänsten.

Senast den 21 maj 2025 ska kommissionen, genom genomförandeaakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för kvalificerade elektroniska arkiveringstjänster.

4.9.4 Elektroniska liggare

Elektroniska liggare definieras enligt artikel 3.52 i den reviderade eIDAS-förordningen som en sekvens av elektroniska dataloggar som säkerställer dataintegriteten och riktigheten i dessa loggars kronologiska ordning. Av artikel 3.54 följer att dataloggar definieras som elektroniska uppgifter som registrerats med tillhörande metadata som stöder behandlingen av dessa data. I artikel 45k regleras det rättsliga erkännandet av elektroniska liggare. Enligt artikel 45k.2 ska dataloggar i en kvalificerad elektronisk liggare omfattas av en presumtion om deras unika och korrekta sekventiella kronologiska ordningsföljd och deras integritet.

Kraven på kvalificerade elektroniska liggare finns i artikel 45l och de ska möta följande krav:

- a) De ska skapas och förvaltas av en eller flera kvalificerade tillhandahållare av betrodda tjänster.
- b) De ska fastställa ursprunget till dataloggarna i liggaren.

- c) De ska säkerställa unik sekventiell kronologisk ordning för data-loggarna i liggaren.
- d) De ska registrera data på ett sådant sätt att alla senare ändringar av uppgifterna omedelbart kan upptäckas, varvid deras integritet säkerställs över tid.

Kommissionen ska senast den 21 maj 2025 enligt artikel 451.3 genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för de krav som fastställs i punkt 1 i denna artikel.

4.10 Tillhandahållare av betrodda tjänster

4.10.1 Kvalificerade och icke-kvalificerade tillhandahållare

Tillhandahållare av betrodda tjänster har en central roll i eIDAS-regelverket. En tillhandahållare av betrodda tjänster är enligt artikel 3.19 i eIDAS-förordningen en fysisk eller juridisk person som tillhandahåller en eller flera betrodda tjänster, antingen i egenskap av kvalificerade eller icke-kvalificerade tillhandahållare av betrodda tjänster. Som definitionen anger kan en tillhandahållare vara kvalificerad eller icke-kvalificerad. Skillnaden mellan de båda framgår bl.a. av artikel 3.20, där det anges att en kvalificerad tillhandahållare är en tillhandahållare av betrodda tjänster som tillhandahåller en eller flera kvalificerade betrodda tjänster och som beviljats status som kvalificerad av tillsynsorganet.

4.10.2 Säkerhetskrav och krav på incidentrapportering

Säkerhetskraven på kvalificerade och icke-kvalificerade tillhandahållare av betrodda tjänster regleras dels i det s.k. NIS2-direktivet³⁴, dels i den reviderade eIDAS-förordningen. Enligt NIS2-direktivet är icke-kvalificerade tillhandahållare av betrodda tjänster viktiga enheter medan kvalificerade tillhandahållare av betrodda tjänster är väsentliga en-

³⁴ Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS2-direktivet) (Text av betydelse för EES).

heter.³⁵ Kraven på cybersäkerhet och riskhantering finns i artikel 21 i NIS2-direktivet:

1. Medlemsstaterna ska säkerställa att väsentliga och viktiga entiteter vidtar lämpliga och proportionella tekniska, driftsrelaterade och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverks- och informationssystem som de använder för sin verksamhet eller för att tillhandahålla sina tjänster och för att förhindra eller minimera incidenters påverkan på mottagarna av deras tjänster och på andra tjänster.

Med beaktande av de senaste, och i tillämpliga fall, relevanta europeiska och internationella standarder samt genomförandekostnaderna, ska de åtgärder som avses i första stycket säkerställa en nivå på säkerheten i nätverks- och informationssystem som är lämplig i förhållande till den föreliggande risken. Vid bedömningen av dessa åtgärders proportionalitet ska vederbörlig hänsyn tas till entitetens grad av riskexponering, entitetens storlek samt sannolikheten för att incidenter inträffar och deras allvarlighetsgrad, inbegripet deras samhälleliga och ekonomiska konsekvenser.

2. De åtgärder som avses i punkt 1 ska baseras på en allriskansats som syftar till att skydda nätverks- och informationssystem och dessa systems fysiska miljö från incidenter, och ska minst inbegripa

- a) strategier för riskanalys och informationssystemens säkerhet,
- b) incidenthantering,
- c) driftskontinuitet, exempelvis hantering av säkerhetskopiering och katastrofhantering, och krishantering,
- d) säkerhet i leveranskedjan, inbegripet säkerhetsaspekter som rör förbindelserna mellan varje entitet och dess direkta leverantörer eller tjänsteleverantörer,
- e) säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem, inbegripet hantering av sårbarheter och sårbarhetsinformation,
- f) strategier och förfaranden för att bedöma effektiviteten i riskhanteringsåtgärderna för cybersäkerhet,
- g) grundläggande praxis för cyberhygien och utbildning i cybersäkerhet,
- h) strategier och förfaranden för användning av kryptografi och, när så är lämpligt, kryptering,
- i) personalsäkerhet, strategier för åtkomstkontroll och tillgångsförvaltning,
- j) användning inom entiteten, när så är lämpligt, av lösningar för multifaktorautentisering eller kontinuerlig autentisering, säkrade röst-, video- och textkommunikationer och säkrade nödkommunikationssystem.

Utöver bestämmelserna i NIS2-direktivet pågår arbete med en genomförandeakt som fastställer de tekniska och metodologiska specifikationerna för punkterna ovan. Denna genomförandeakt ska vara antagen senast den 17 oktober 2024 och omfattar kraven på tillhandahållare

³⁵ A.a. artikel 3.1 b) respektive artikel 3.2.

av betrodda tjänster.³⁶ Utredningen om genomförande av NIS2- och CER-direktiven har i sitt delbetänkande³⁷ föreslagit en cybersäkerhetslag som bl.a. reglerar riskhanteringsåtgärder och incidentrapportering.³⁸ Den reviderade eIDAS-förordningen kompletterar NIS2-direktivet genom att ställa säkerhetskrav som är mer specifika för de betrodda tjänster som tillhandahålls och omfattar andra områden än nät- och informationssystem som behövs för att tillhandahålla tjänster. Mer generella säkerhetskrav finns i artikel 19a avseende icke-kvalificerade tillhandahållare av betrodda tjänster och i artikel 24.2 fa) avseende kvalificerade tillhandahållare av betrodda tjänster som utfärdar kvalificerade certifikat. Bestämmelserna är likalydande i sin utformning och enbart entiteten som regleras skiljer sig. Tillhandahållare av betrodda tjänster ska:

- a) ha lämpliga policyer och vidta motsvarande åtgärder för att hantera rättsliga, affärsmässiga, operativa och andra direkta eller indirekta risker för tillhandahållandet av kvalificerade betrodda tjänster; trots bestämmelserna i artikel 21 i direktiv Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS2-direktivet) ska dessa åtgärder innefatta åtminstone
 - i) åtgärder avseende registrering och onboarding-förfaranden för en tjänst,
 - ii) åtgärder avseende förfarandemässiga eller administrativa kontroller,
 - iii) åtgärder avseende förvaltning och genomförande av tjänster.

Utöver säkerhetsbestämmelser regleras även incidentrapporteringen för icke-kvalificerade och kvalificerade tillhandahållare av betrodda tjänster främst i NIS2-direktivet³⁹ men även till viss del i den reviderade eIDAS-förordningen. I detta fall avser rapporteringen överträdelser av de specifika kompletterande kraven på säkerhet som finns i förordningen.

³⁶ Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS2-direktivet), artikel 21.5.

³⁷ *Nya regler om cybersäkerhet* (SOU 2024:18).

³⁸ A.a. s. 41 ff.

³⁹ Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet), artikel 23.

4.10.3 Skillnader i skadeståndsansvar och bevisbörda

Av artikel 13, som delvis ändrats i den reviderade eIDAS-förordningen, framgår att tillhandahållare av betrodda tjänster omfattas av skadeståndsansvar för skada som åsamkats en fysisk eller juridisk person avsiktligt eller på grund av oaktsamhet genom underlåtenhet att uppfylla kraven i förordningen. Placeringen av bevisbördan skiljer sig åt beroende på om tillhandahållaren är kvalificerad eller inte. Presumtionen vid skada är att bevisbördan ligger på tillhandahållaren om denne är kvalificerad. Det är således den kvalificerade tillhandahållaren som ska bevisa att den skada som uppstått har uppstått utan dennes avsikt eller oaktsamhet. Om tillhandahållaren är icke-kvalificerad vilar i stället bevisbördan på den som gör gällande att skada har uppstått.

4.10.4 Krav på kvalificerade tillhandahållare

Som tidigare nämnts omfattas kvalificerade tillhandahållare av betrodda tjänster av betydligt fler krav än icke-kvalificerade. För att få status som kvalificerad tillhandahållare krävs enligt artikel 21.1 en anmälan till ett tillsynsorgan. Tillhandahållaren ska i samband med anmälan även lämna in en rapport om överensstämmelsebedömning som utfärdats av ett organ för bedömning av överensstämmelse. Bedömningen av överensstämmelse ska omfatta både tillhandahållaren som sådan och de betrodda tjänster som tillhandahållaren vill ska vara kvalificerade. Ett sådant organ ska enligt artikel 3.18 vara ackrediterat för att göra bedömningar av sådana tillhandahållare och de tjänster de tillhandahåller. I Sverige ackrediterar den statliga myndigheten Styrelsen för ackreditering och teknisk kontroll (Swedac) sådana organ.

Tillsynsorganet ska enligt artikel 21.2 kontrollera om tillhandahållaren och de betrodda tjänster som denne tillhandahåller uppfyller kraven i förordningen. Om tillsynsorganet kommer fram till att tillhandahållaren och de betrodda tjänster som denne tillhandahåller uppfyller kraven i förordningen ska organet bevilja tillhandahållaren status som kvalificerad tillhandahållare av betrodda tjänster. Det samma gäller de tjänster som den tillhandahåller. I samband med det ska den aktuella medlemsstatens förteckning över kvalificerade tillhandahållare och betrodda tjänster, som avses i artikel 22.1 i förordningen, uppdateras så att tillhandahållaren och tjänsterna förs upp på förteckningen. Kommissionen ska enligt artikel 21.4 inom 12 måna-

der från förordningens ikraftträdande anta genomförandeakter avseende format och förfaranden på detta område.

Uttryckliga krav som kvalificerade tillhandahållare har att förhålla sig till finns i artikel 24. Kraven avser primärt tillhandahållaren som sådan och flera av dem har starka kopplingar till de kvalificerade certifikat som utfärdas. Nedan följer några exempel på dessa krav. Kvalificerade tillhandahållare ska bl.a. använda tillförlitliga system och produkter som är skyddade mot ändringar och säkerställa den tekniska säkerheten och tillförlitligheten hos den process som stöds av systemen (artikel 24.2 e). De ska också ha personal, och i förekommande fall underleverantörer, som har den sakkunskap, tillförlitlighet samt de erfarenheter och kvalifikationer som behövs och som har genomgått lämplig utbildning om regler för säkerhet och skydd för personuppgifter (artikel 24.2 b). Vidare ska kvalificerade tillhandahållare förfoga över tillräckliga ekonomiska medel och/eller skaffa sig lämplig ansvarsförsäkring i enlighet med nationell rätt, detta med anledning av risken för ansvar vid skador (artikel 24.2 c). Tillhandahållare som utfärdar kvalificerade certifikat ska bl.a. upprätta en certifikatdatabas som hålls uppdaterad (artikel 24.2 k). Om de beslutar att återkalla ett certifikat ska ett sådant återkallande registreras i certifikatdatabasen och offentliggöras i god tid och senast inom 24 timmar efter mottagandet av begäran (artikel 24.3).

Enligt artikel 20.1 ska kvalificerade tillhandahållare minst en gång vartannat år och på egen bekostnad granskas av ett organ för bedömning av överensstämmelse. Syftet med granskningen är att bekräfta att tillhandahållaren och de kvalificerade betrodda tjänsterna uppfyller kraven i förordningen. Den rapport som bedömningen resulterar i ska överlämnas till tillsynsorganet.

4.10.5 Tillsyn

Utöver tillhandahållare av betrodda tjänster har de nationella tillsynsorganen en viktig roll i den reviderade eIDAS-förordningen. Enligt artikel 46b ska medlemsstaterna utse ett eller flera tillsynsorgan som är etablerat inom deras territorium som ska ansvara för tillsynsuppgifter i den medlemsstat som utsett organet. Det är även möjligt att utse ett tillsynsorgan som är etablerat i en annan medlemsstat, efter ömsesidig överenskommelse med den medlemsstaten. Den reviderade

eIDAS-förordningen ställer betydligt högre krav på tillsyn över kvalificerade tillhandahållare och betrodda tjänster än tillhandahållare och betrodda tjänster som är icke-kvalificerade. När det gäller kvalificerade tillhandahållare och betrodda tjänster ska organen aktivt utöva tillsyn i enlighet med de bestämmelser som finns i förordningen, för att se till att tillhandahållarna och tjänsterna uppfyller kraven i förordningen. För icke-kvalificerade tillhandahållare och tjänster är tillsynen emellertid händelsestyrd, således efter rapporterad incident eller vid objektiv misstanke om att reglerna inte efterlevs.

Vissa av tillsynsorganens uppgifter har nämnts i tidigare avsnitt, såsom beviljandet av status om kvalificerad tillhandahållare och hantering av säkerhetsincidenter. Organen får dessutom för bedömning av överensstämmelse när som helst granska eller begära att ett organ för bedömning av överensstämmelse gör en överensstämmelsebedömning av de kvalificerade tillhandahållarna för att bekräfta att de och de kvalificerade betrodda tjänster som tillhandahåller uppfyller kraven i förordningen. Tillsynsorganet behöver även samverka med tillsynsmyndigheter som ansvarar för betrodda tjänster enligt NIS2-direktivet gällande såväl etablering av kvalificerade tillhandahållare som rapporterade incidenter avseende tillhandahållare av betrodda tjänster och de tjänster de tillhandahåller.

Tillsynsorganen i medlemsstaterna ska samarbeta och ge varandra ömsesidigt bistånd när det behövs, exempelvis genom att förse ett annat organ med information eller bistå med tillsynsåtgärder. Det finns även ett forum för tillsynsorganen, Forum of European Supervisory Authorities for trust service providers (FESA) som bl.a. syftar till att främja samarbetet mellan organen. Utöver tillsynsorgan från EU:s medlemsstater deltar också tillsynsorgan från andra länder i forumet, exempelvis Albanien och Serbien. Samarbete sker även inom Enisas gruppering European Competent Authorities for Trust Services (ECATS).

4.10.6 Sanktioner

Enligt artikel 16.1 i den reviderade eIDAS-förordningen ska medlemsstaterna fastställa bestämmelser om de sanktioner som ska tillämpas vid överträdelser av förordningen. Sanktionerna ska vara effektiva, proportionella och avskräckande.

Av artikel 16.2 framgår att överträdelser av bestämmelser i förordningen som begås av kvalificerade eller icke-kvalificerade tillhandahållare av betrodda tjänster ska förenas med sanktionsavgifter (se mer om sanktionsavgifter i avsnitt 6.6.7–6.6.12).

4.10.7 Förteckning över tillhandahållare och betrodda tjänster

Enligt artikel 22 i eIDAS-förordningen ska varje medlemsstat upprätta, underhålla och offentliggöra förteckningar med uppgifter om kvalificerade tillhandahållare av betrodda tjänster som den ansvarar för, tillsammans med uppgifter om de kvalificerade betrodda tjänster som dessa tillhandahåller. Dessa tillitsförteckningar benämns som ”trusted list” i den engelska språkversionen av förordningen och det är även vanligt att den engelska termen används i Sverige.

Medlemsstaterna ska på ett säkert sätt upprätta, underhålla och offentliggöra elektroniskt undertecknade eller förseglade förteckningar i en form som lämpar sig för automatiserad behandling. Kommissionen har i ett genomförandebeslut fastställt tekniska minimispecifikationer och format för förteckningarna.⁴⁰ Syftet med förteckningarna är att det ska gå att kontrollera vilka tillhandahållare på marknaden som är kvalificerade samt se vilka betrodda tjänster de tillhandahåller.

4.11 Rättslig verkan av betrodda tjänster

Förordningen innehåller ett flertal bestämmelser om rättslig verkan. Till att börja med föreskrivs i artikel 25.1, 35.1, 41.1 respektive 46 att elektroniska underskrifter, elektroniska stämplor, elektroniska tidsstämplingar och elektroniska dokument inte får förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att de har elektronisk form eller, med undantag för elektroniska dokument, för att de inte lever upp till kraven för att vara kvalificerade.

⁴⁰ Kommissionens genomförandebeslut (EU) 2015/1505 av den 8 september 2015 om fastställande av tekniska minimispecifikationer och format rörande förteckningar över betrodda tjänsteleverantörer i enlighet med artikel 22.5 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden (Text av betydelse för EES).

För elektroniska tjänster för rekommenderade leveranser gäller enligt artikel 43.1 att uppgifter som sänds och tas emot genom en sådan tjänst inte får förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att de har elektronisk form eller för att de inte uppfyller kraven på den kvalificerade elektroniska tjänsten för rekommenderade leveranser. Innebörden av den senare skrivningen är något svårtolkad. Den torde emellertid innebära att uppgifterna inte får förvägras rättslig verkan enbart på grund av att tjänsten som de har sänts eller tagits emot med inte är kvalificerad.

För vissa tjänster finns dessutom egna bestämmelser om tjänsterna är kvalificerade. I artikel 25.2 föreskrivs att en kvalificerad elektronisk underskrift ska ha motsvarande rättsliga verkan som en handskriven underskrift. Detta innebär emellertid inte att en kvalificerad elektronisk underskrift kan ersätta egenhändigt undertecknande när ett sådant formkrav finns i nationell rätt.⁴¹

Vidare finns i förordningen för kvalificerade tjänster för elektroniska stämplor (artikel 35.2), elektroniska tidsstämplingar (artikel 41.2) och elektroniska tjänster för rekommenderade leveranser (artikel 43.2) också regler om presumtion om integritet och korrekthet. En kvalificerad elektronisk stämpel ska t.ex. enligt ovan nämnd artikel omfattas av en presumtion om integritet hos de uppgifter som den kvalificerade elektroniska stämpeln är kopplad till och om att de har korrekt ursprung. Vad gäller rättslig verkan av nya betrodda tjänster, se avsnitt 4.9.

4.11.1 Erkännande av betrodda tjänster från andra länder

I den reviderade eIDAS-förordningen finns i artikel 24a.1 och 24a.3 bestämmelser om att kvalificerade elektroniska underskrifter och stämplor som baseras på ett kvalificerat certifikat som utfärdats i en medlemsstat ska erkännas som kvalificerad elektronisk underskrift eller stämpel i alla andra medlemsstater.

Anordningar för skapande av kvalificerade elektroniska underskrifter och stämplor som certifieras i en medlemsstat ska godtas som sådana anordningar i alla medlemsstater (artikel 24a.2).

⁴¹ Se mer om tolkningen av innebörden av denna artikel i *Vem kan man lita på? – Enkel och ändamålsenlig användning av betrodda tjänster i den offentliga förvaltningen* (SOU 2021:9) s. 102 f.

Samma erkännande gäller när kvalificerade elektroniska underskrifter och stämplat skapas med kvalificerade tjänster för förvaltning av anordningar för skapande av elektroniska underskrifter på distans så såväl underskrifter och stämplat som anordningar ska erkännas av alla medlemsstater.

Enligt artikel 24a.4 och 24a.5 ska kvalificerade tjänster för validering av kvalificerade underskrifter och stämplat respektive kvalificerade tjänster för bevarande av kvalificerade elektroniska underskrifter och stämplat erkännas i alla medlemsstater. Detsamma gäller för en kvalificerad elektronisk tidsstämpling enligt artikel 24a.6.

Ett kvalificerat certifikat för autentisering av webbplatser, en kvalificerad elektronisk tjänst för rekommenderade leveranser, ett kvalificerat elektroniskt attributsintyg, en kvalificerad elektronisk arkiveringstjänst och en kvalificerad elektronisk liggare som tillhandahålls i en medlemsstat ska erkännas som kvalificerade sådana tjänster i alla medlemsstater i enlighet med artikel 24a.7–11.

För erkännande av betrodda tjänster som tillhandahålls i tredje land finns i artikel 14 bestämmelser om hur sådana kan godtas.

5 Nationell reglering av elektronisk identifiering och betrodda tjänster

5.1 Svenska kompletterande bestämmelser

De nationella författningsåtgärder som i tidigare lagstiftningsärenden har bedömts vara nödvändiga till stöd för eIDAS-förordningens tillämpning i Sverige finns i lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering (härefter kompletteringslagen) och i förordningen (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering (härefter kompletteringsförordningen).

I kompletteringslagen delegeras i huvudsak olika uppgifter som anges i eIDAS-förordningen kopplade till ackreditering, certifiering och tillsyn, främst i fråga om betrodda tjänster (2–5 §§). I 2 § kompletteringslagen anges vidare att ytterligare bestämmelser om ackreditering av sådana organ för bedömning av överensstämmelse som ska granska kvalificerade tillhandahållare av betrodda tjänster finns i förordningen (EG) nr 765/2008¹ och i lagen (2011:791) om ackreditering och teknisk kontroll. I enlighet med eIDAS-förordningen finns i kompletteringslagen även bestämmelser om sanktioner för överträdelser av förordningen (6 §), och regler om överklagande av tillsynsmyndighetens beslut (8 §).

Med stöd av kompletteringslagen och kompletteringsförordningen får dessutom Post- och telestyrelsen (PTS), Myndigheten för digital förvaltning (Digg) och Myndigheten för samhällsskydd och beredskap (MSB) meddela föreskrifter inom vissa områden. Myndigheterna får

¹ Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93 (Text av betydelse för EES).

föreskriva t.ex. om krav för ackreditering av organ för överensstämmelsebedömning, hur sådana bedömningar ska göras och avrapporteras, om certifiering av anordningar för skapande av kvalificerade elektroniska underskrifter och anordningar för skapande av kvalificerade elektroniska stämplat, om säkerhetsegenskaper som sådana anordningar ska uppfylla samt om förfarandet och kraven för anslutning till den svenska förbindelsepunkten (noden) för inkommande gränsöverskridande elektronisk identifiering, och om vilka krav som ska gälla för att ett system för elektronisk identifiering ska få anmälas för gränsöverskridande elektronisk identifiering.

Vid Försvarets materielverk finns ett nationellt certifieringsorgan för it-säkerhet i produkter och system (CSEC). Av 5 § andra stycket förordningen (2007:854) med instruktion för Försvarets materielverk framgår att CSEC ska ansvara för certifiering av anordningar för skapande av kvalificerade elektroniska underskrifter och anordningar för kvalificerade elektroniska stämplat enligt artikel 30 och 39 i eIDAS-förordningen.

5.2 Tillsyn

Enligt eIDAS-förordningens artikel 17.1 i dess tidigare lydelse är medlemsstaterna skyldiga att utse ett tillsynsorgan som är etablerat inom deras territorium som ska ansvara för tillsynsuppgifter i den medlemsstat som utsett organet. Det är även möjligt att utse ett tillsynsorgan som är etablerat i en annan medlemsstat, efter ömsesidig överenskomelse med den medlemsstaten.

I Sverige är PTS tillsynsorgan (4 § kompletteringsförordningen). Tillsynsansvaret är begränsat till betrodda tjänster. eIDAS-förordningen ställer högre krav på tillsyn över kvalificerade tillhandahållare och betrodda tjänster än tillhandahållare och betrodda tjänster som är icke-kvalificerade. När det gäller de förra ska aktiv tillsyn utövas i enlighet med de bestämmelser som finns i förordningen, för att se till att tillhandahållarna och tjänsterna uppfyller föreskrivna krav. För icke-kvalificerade tillhandahållare och tjänster är tillsynen i stället händelsestyrd, dvs. förutsätter att det finns en rapporterad incident eller en misstanke om att reglerna inte efterlevs. Den närmare innebörden av myndighetens tillsynsuppgifter redovisas i avsnitt 4.10.5. Tillsynsorganen i medlemsstaterna ska samarbeta och ge varandra ömsesidigt

bistånd när det behövs, exempelvis genom att förse ett annat organ med information eller bistå med tillsynsåtgärder. Det finns även ett forum för tillsynsorganen, Forum of European Supervisory Authorities for trust service providers (FESA) som bl.a. syftar till att främja samarbetet mellan organen.

Inom ramen för sitt ansvar att främja användningen av elektronisk identifiering har Digg enligt sin myndighetsinstruktion bl.a. ansvar för att förvalta och utveckla tillitsramverket för kvalitetsmärket Svensk e-legitimation (3 § 2 förordningen [2018:1486] med instruktion för Myndigheten för digital förvaltning). En e-legitimation för vilken dess utfärdare har ansökt om kvalitetsmärket granskas av Digg enligt kraven i det svenska tillitsramverket. Digg har dock inte något tillsynsansvar över utfärdare av e-legitimationer i förhållande till eIDAS-förordningen.² Se mer om tillsyn beträffande nationellt utfärdade e-legitimationer i avsnitt 6.6.6.

² Omständigheten att utfärdare av e-legitimationer står under enbart begränsad tillsyn, uppdelad på flera statliga myndigheter har problematiserats, bl.a. i betänkandet *En säker och tillgänglig statlig e-legitimation* (SOU 2023:61), s. 180 ff.

6 Överväganden och förslag

6.1 Behovet av ytterligare kompletterande bestämmelser till den reviderade eIDAS-förordningen

Utredningens bedömning: EU:s reviderade förordning om elektronisk identifiering bör kompletteras med ytterligare nationella bestämmelser som säkerställer bl.a. att Sverige fullt ut uppfyller kravet på att det tillhandahålls minst en europeisk digital identitetsplånbok i enlighet med förordningen.

Skälen för utredningens bedömning

En EU-förordning är bindande i sin helhet och direkt tillämplig i varje medlemsstat. En sådan rättsakt varken ska eller får genomföras i eller omvandlas till nationell rätt. Några särskilda åtgärder för att införliva de materiella bestämmelserna i den reviderade EU-förordningen om elektronisk identifiering med nationell rätt får alltså inte vidtas. Det är bara om svensk rätt kan anses strida mot förordningen, om förordningen föreskriver en skyldighet eller möjlighet att vidta lagstiftningsåtgärder på det nationella planet, eller om det behövs andra nationella åtgärder till stöd för förordningens syfte som ändringar i svensk rätt aktualiseras.

När det gäller den reviderade eIDAS-förordningen behöver den kompletteras med nationella bestämmelser som säkerställer att Sverige fullt ut uppfyller kravet på att minst en europeisk digital identitetsplånbok tillhandahålls i enlighet med förordningen.

Förordningen förutsätter också att medlemsstaterna vidtar vissa nationella åtgärder. Det handlar om att utse bedömningsorgan med uppdrag att certifiera *dels* europeiska digitala identitetsplånböcker

och de system för elektronisk identifiering inom ramen för vilka de tillhandahålls, dels sådana e-legitimationssystem som ska genomgå förordningens anmälningsförfarande för gränsöverskridande användning (artikel 5c.1 respektive 12a.1). Vidare ska medlemsstaterna utse organ som ansvarar för register över förlitande parter som avser att förlita sig på europeiska digitala identitetsplånböcker (artikel 5b.1 i förening med artikel 5a.18 a). Det handlar också om att säkerställa att överträdelser av eIDAS-förordningen träffas av bestämmelser som föreskriver effektiva, proportionella och avskräckande sanktioner (artikel 16). Till skillnad från tidigare fastslås att överträdelse som begås av kvalificerade och icke-kvalificerade tillhandahållare av betrodna tjänster ska medföra sanktionsavgifter.

Den reviderade eIDAS-förordningen ger i vissa delar medlemsstaterna även möjlighet att vidta åtgärder. Av artikel 5a.7 följer att medlemsstaterna, i enlighet med nationell rätt, får föreskriva ytterligare funktioner för de europeiska digitala identitetsplånböckerna, inbegripet interoperabilitet med befintliga nationella medel för elektronisk identifiering.

Ett annat exempel på utrymme för nationell reglering har anknytning till reglerna om att den europeiska digitala identitetsplånboken ska vara kostnadsfri för fysiska personer (artikel 5a.13). Som utgångspunkt ska identitetsplånboken ge alla fysiska personer möjlighet att kostnadsfritt underteckna med kvalificerade elektroniska underskrifter (artikel 5a.5 g). Ifrågavarande användning ska dock kunna begränsas till sådan för icke-yrkesmässiga ändamål (artikel 5a.5 andra stycket). Även beträffande tillämpning av dataskyddsåtgärder finns visst utrymme för medlemsstaterna att föreskriva om ytterligare specificeringar (artikel 5a.17). Vi återkommer till dessa frågor i det följande.

Avslutningsvis kan tilläggas att det på vissa ställen i den reviderade eIDAS-förordningen även hänvisas till reglering i nationell rätt. Exempelvis fastslås det i artikel 2.3, med visst förtydligande, att förordningen inte påverkar unionsrätt eller nationell rätt som avser ingående av avtal och deras giltighet eller andra rättsliga eller förfarandemässiga skyldigheter avseende form, eller sektorspecifika krav avseende form. För svenskt vidkommande finns anledning att driva på digitaliseringsarbetet inom offentlig förvaltning. Med hänsyn till vårt uppdrags tidsram finns dock inte utrymme för överväganden om exempelvis författningskrav om digitaliserad ärendehandläggning.

6.2 Nya och ändrade nationella bestämmelser med anledning av den reviderade eIDAS-förordningen

Utredningens förslag: Nödvändiga nationella bestämmelser införs i den befintliga lagen respektive förordningen med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

De hänvisningar till EU-förordningen som finns i lagen ska, med undantag för bestämmelsen om sanktionsavgift, avse förordningen i den vid varje tidpunkt gällande lydelsen.

Tillägg ska göras i respektive myndighetsinstruktion för de myndigheter som av regeringen ges ett nytt eller utökat ansvar i egenskap av

- tillhandahållare av den europeiska digitala identitetsplånboken,
- tillhandahållare av sådana elektroniska attesteringar av uppgifter för personidentifiering som ska kunna kopplas till en europeisk digital identitetsplånbok, och
- ansvarigt organ att utöva tillsyn över ramverket för den europeiska digitala identitetsplånboken.

Utredningens bedömning: Det föreligger i nuläget inget behov av lagstiftningsåtgärd vad gäller hänvisningar till EU:s förordning om elektronisk identifiering i andra svenska författningar.

Skälen för utredningens förslag och bedömning

I lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering (kompletteringslagen) och förordningen (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering (kompletteringsförordningen) är det lämpligt att reglera hur den europeiska digitala identitetsplånboken ska tillhandahållas (se avsnitt 6.3.1). Dessa författningar lämpar sig också för reglering av vilka aktörer som ska ansvara för tillhandahållandet av elektroniska attesteringar av uppgifter för personidentifiering att koppla till identitetsplånboken (se avsnitt 6.3.3). Likaså ska det i kompletteringslagen och kompletteringsförordningen införas bestämmelser om dels ansvar för certifiering av den europeiska

digitala identitetsplånboken såväl som system för elektronisk identifiering, dels ansvar för tillsyn över tillhandahållare av sådana identitetsplånböcker och för registret över förlitande parter.

För de myndigheter som utses av regeringen till tillhandahållare av dels identitetsplånboken, dels uppgifter om personidentifiering och till tillsynsorgan ska tillägg göras om dessa nya uppgifter i respektive myndighets instruktion (se avsnitten 6.3.1, 6.3.3, 6.6.1 och 6.6.2). Såvitt gäller ansvar som certifieringsorgan, är det dock lämpligare att i stället reglera detta i kompletteringsförordningen (se avsnitt 6.3.7).

I kompletteringslagen och kompletteringsförordningen införs lämpligen också nödvändiga bestämmelser om behandling av personuppgifter för tillhandahållandet av den europeiska digitala identitetsplånboken (se avsnitt 6.3.9) samt reglering av möjligheten för tillsynsmyndigheten över tillhandahållare av betrodda tjänster att påföra sanktionsavgifter i enlighet med den reviderade eIDAS-förordningen (se avsnitt 6.6.7). Med anledning av de relativt sett många nya bestämmelser som ska införas i dessa författningar ges samtidigt vissa befintliga bestämmelser nya beteckningar i syfte att skapa en mer överskådlig struktur.¹

I ett antal svenska författningar förekommer hänvisningar till eIDAS-förordningen, huvudsakligen till definitionen av avancerad elektronisk underskrift i artikel 3. Dessa hänvisningar är s.k. statiska hänvisningar (se bilaga 3 till detta betänkande). Det gäller även för den befintliga hänvisningen till eIDAS-förordningen i kompletteringslagen, men däremot inte i fråga om kompletteringsförordningen (eller för myndighetsinstruktionerna för Myndigheten för digital förvaltning [Digg] och Post- och telestyrelsen [PTS]).

Hänvisningar till EU-rättsakter i författningar kan, som framgått, göras antingen statiska eller dynamiska. En statisk hänvisning innebär att hänvisningen avser EU-rättsakten i en viss angiven lydelse; som i nu förekommande fall i kompletteringslagen, till eIDAS-förordningen ”i dess ursprungliga lydelse”. En följd av denna hänvisningsteknik är att den nationella författningen normalt behöver ändras varje gång EU-bestämmelsen ändras. En dynamisk hänvisning innebär däremot att hänvisningen avser EU-rättsakten i den vid varje tidpunkt gällande lydelsen.

¹ En sökning i Svensk författningssamling (SFS) visar att det finns en lagrumshänvisning till kompletteringslagen: 1 § förordningen (2016:602) om finansiering av Post- och telestyrelsens verksamhet.

Som framgår av avsnitt 4.10.6 och som närmare behandlas i avsnitten 6.6.7–6.6.12 föreskrivs i den reviderade eIDAS-förordningen att medlemsstaterna ska säkerställa att regelöverträdelser som begås av kvalificerade och icke-kvalificerade tillhandahållare av betrodda tjänster medför sanktionsavgifter. De sanktionsbestämmelser som vi, till följd därav, föreslår ska införas i kompletteringslagen bör innehålla statiska hänvisningar till förordningen med hänsyn till behovet av förutsebarhet i fråga om vilka överträdelser som kan leda till sanktioner.²

För att säkerställa att eventuella ändringar i eIDAS-förordningen kan få omedelbart genomslag är det lämpligt att övriga hänvisningar i kompletteringslagen är dynamiska. Den befintliga statiska hänvisningen i 1 § ska därmed ändras.

När det gäller övriga lagar och förordningar med statiska hänvisningar till eIDAS-förordningens definition av avancerad elektronisk underskrift i artikel 3 föreligger i nuläget, trots revisionen av eIDAS-förordningen, inget behov av lagstiftningsåtgärd. Definitionen i fråga är densamma i den ursprungliga och den reviderade eIDAS-förordningen. För det fall det anses påkallat att ersätta den statiska hänvisningen till en dynamisk kan en ändring göras i samband med att ifrågasvarande författningar är föremål för ett lagstiftningsärende i även andra avseenden.

6.3 Den europeiska digitala identitetsplånboken

6.3.1 Tillhandahållare av den europeiska digitala identitetsplånboken

Utredningens förslag: Den statliga myndighet som regeringen bestämmer ska tillhandahålla den europeiska digitala identitetsplånboken till fysiska och juridiska personer i enlighet med EU:s reviderade förordning om elektronisk identifiering (tillhandahållande myndighet).

Efter anmälan, granskning och godkännande får även privata aktörer tillhandahålla en certifierad europeisk digital identitetsplånbok till fysiska och juridiska personer. För godkännande krävs

² Se t.ex. lagrådsremissen den 2 maj 2024 med kompletterande bestämmelser till EU:s förordning om digitala tjänster, s. 30 f.

att tillhandahållaren kan uppfylla villkoren för den europeiska digitala identitetsplån-boken enligt den reviderade EU-förordningen och rättsakter som meddelats i anslutning till förordningen samt kraven i lagen med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering och föreskrifter som meddelats med stöd av lagen.

Ansvarig för granskning och godkännande ska vara den myndighet som av regeringen utsetts som tillhandahållare av den europeiska digitala identitetsplån-boken. Den tillhandahållande myndigheten ska underrätta tillsynsmyndigheten över tillhandahållare av den europeiska digitala identitetsplån-boken om det finns anledning att anta att villkoren för ett godkännande inte längre är uppfyllda.

Regeringen eller den myndighet som regeringen bestämmer ska meddela föreskrifter om anmälnings- och granskningsförfarandet och de villkor som ska gälla för ett godkännande som tillhandahållare av den europeiska digitala identitetsplån-boken.

För tillhandahållande av den europeiska digitala identitetsplån-boken till juridiska personer får en avgift tas ut av den tillhandahållande myndigheten.

Utredningens bedömning: Myndigheten för digital förvaltning är bäst lämpad för uppgiften att tillhandahålla den digitala europeiska identitetsplån-boken för såväl fysiska som juridiska personer.

Skälen för utredningens förslag och bedömning

En öppen modell för certifierade europeiska digitala identitetsplån-böcker

I vårt uppdrag ingår att utreda hur det kan säkerställas att en kostnadseffektiv europeisk digital identitetsplån-bok i enlighet med den reviderade eIDAS-förordningen ska utfärdas.

Förordningen tillåter, som framgått, att identitetsplån-boken utfärdas a) direkt av en medlemsstat, b) på uppdrag av en medlemsstat eller c) oberoende av en medlemsstat men erkänd av ifrågavarande medlemsstat (se artikel 5a.2 och skäl 16 i förordningens ingress samt jfr artikel 7 om berättigande till anmälan av system för elektronisk identifiering).

Digg har föreslagit att en statlig myndighet får ett författningsreglerat uppdrag att utfärda och tillhandahålla identitetsplånböcker med föreskrivna funktioner enligt eIDAS-förordningen. Vid sidan av en statligt tillhandahållen europeisk digital identitetsplånbok bör enligt Digg även privata aktörer tillåtas att erbjuda sådana plånböcker.³

Digg har identifierat att det finns ett intresse hos privata aktörer att eventuellt erbjuda identitetsplånböcker.⁴ Denna bild stämmer överens med vad som framkommit vid utredningens kontakter med aktörer inom den privata sektorn. Det har i dessa sammanhang bekräftats att det finns förutsättningar att dra nytta av och att det kan komma att finnas möjligheter att bygga vidare på erfarenheter av befintliga medel för elektronisk identifiering och bakomliggande infrastruktur (jfr skäl 8 i den reviderade eIDAS-förordningens ingress).

Som tidigare redovisats förutsätter den reviderade eIDAS-förordningen att det finns tillgång till minst en digital europeisk identitetsplånbok i varje medlemsland. Detta krav ska vara uppfyllt inom 24 månader från och med ikraftträdande av genomförandeakter som fastställer de tekniska specifikationerna för identitetsplånboken och dess certifiering.⁵ Givet att rättsakterna antas i tid och i anslutning därtill publiceras i Europeiska unionens tidning, ska europeiska digitala identitetsplånböcker finnas tillgängliga senast i december 2026.

Det går inte att garantera att privata aktörer kommer att utveckla och tillhandahålla identitetsplånböcker som är tillgängliga för alla fysiska och juridiska personer i Sverige i enlighet med den reviderade eIDAS-förordningen. För att säkerställa att Sverige inom angiven tidsram uppfyller förordningskravet finns därför behov av att uppdraga åt en statlig myndighet att – vid sidan av eventuella privata aktörer – tillhandahålla en europeisk digital identitetsplånbok. En statligt utfärdad identitetsplånbok kan även öka robustheten i ekosystemet för elektronisk identifiering. I tider av konflikter och ökande cybersäkerhetsshot är det väsentligt att myndigheter och enskilda har tillgång till medel för elektronisk identifiering som staten har rådighet över. Staten har alltså en viktig roll i att öka motståndskraften i systemet men också för att motverka eventuella marknadsmonopol.⁶

³ Myndigheten för digital förvaltning, *Digital plånbok*, 2022-01-11, s. 24 ff.

⁴ Ibid.

⁵ Dessa genomförandeakter ska antas i enlighet med det i artikel 48.2 anvisade förfarandet senast den 21 november 2024, se artikel 5a.1 med hänvisning till artikel 5a.23 och artikel 5c.6.

⁶ Se mer om detta i delbetänkandet *En säker och tillgänglig statlig e-legitimation* (SOU 2023:61), s. 95 ff.

I lagen med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering införs därför en bestämmelse enligt vilken en av regeringen utsedd statlig myndighet ska tillhandahålla en europeisk digital identitetsplånbok (den tillhandahållande myndigheten).

I likhet med Digg förordrar även vi en öppen modell för certifierade europeiska digitala identitetsplånböcker. Med stöd av artikel 5a.2 c i den reviderade eIDAS-förordningen bör därför författningsregleras att även privata aktörer ska kunna erbjuda sådana identitetsplånböcker i enlighet med förordningen efter att ha genomgått ett ansöknings- och granskningsförfarande.

Det är upp till varje medlemsstat att fastställa de villkor och krav som ska gälla för tillhandahållande av en europeisk digital identitetsplånbok på medlemsstatens uppdrag eller med dess erkännande.

Som framgår av det följande gör vi bedömningen att Digg är lämpad för att ansvara för den statligt tillhandahållna europeiska digitala identitetsplånboken. Av anförda skäl för den bedömningen är det ändamålsenligt att samma myndighet också ansvarar för granskning och godkännande av tillhandahållare som avser att erbjuda den europeiska digitala identitetsplånboken (godkända tillhandahållare). Om utfallet av en granskning inte leder till ett godkännande utgör detta ett överklagbart beslut, se vidare avsnitt 6.7.

Om det, efter ett godkännande, framkommer uppgifter som ger anledning att anta att villkoren inte längre är uppfyllda, ska en under rättelse om detta göras till tillsynsmyndigheten över tillhandahållare av den europeiska digitala identitetsplånboken, som har till uppgift att vidta erforderliga åtgärder (se artikel 46a.5). Tillsynsmyndighetens ansvar och befogenheter behandlas närmare i avsnitten 6.6.1 och 6.6.3.

Föreskrifter med villkor för att godkännas som tillhandahållare av den europeiska digitala identitetsplånboken

Det är, som nämnts, upp till varje medlemsstat att fastställa de villkor och krav som ska gälla för tillhandahållande av en europeisk digital identitetsplånbok på medlemsstatens uppdrag eller med dess erkännande. En avgörande förutsättning är att en sådan, av Sverige erkänd, identitetsplånbok uppfyller samtliga krav i den reviderade eIDAS-förordningen och dess genomförandeakter, dvs. samma skyldigheter som direkt enligt förordningen åvilar den myndighet ansvarar för det statligt tillhandahållna europeiska digitala identitetsplånboken. Det är med

denna utgångspunkt som svenska föreskrifter med villkor för godkännande ska utformas.

Därutöver kan det finnas anledning att uppställa vissa ytterligare, främst organisatoriska, krav på tillhandahållaren. Det finns även behov av reglering av anmälnings- och granskningsförfarandet. Dessa bestämmelser bör införas på förordnings- och myndighetsföreskriftsnivå. Regeringen eller den myndighet regeringen bestämmer ska därför bemyndigas att meddela föreskrifter om anmälnings- och granskningsförfarandet och de villkor som bör uppställas för ett godkännande.

Ett godkännande i Sverige som tillhandahållare av den europeiska digitala identitetsplån boken ska alltså villkoras av att den erbjudna identitetsplån boken uppfyller kraven enligt bl.a. artikel 5a i den reviderade EU-förordningen och kommande genomförandeakter och att det kan antas att verksamheten kommer att drivas i enlighet med regelverket för sådana identitetsplån böcker.

I det följande anges exempel på innehåll i föreskrifter om villkor för godkännande som tillhandahållare av den europeiska digitala identitetsplån boken.

Certifieringskravet, som gäller för alla europeiska digitala identitetsplån böcker och de system för elektronisk identifiering inom ramen för vilka de tillhandahålls, regleras direkt i förordningen med tillkommande genomförandeakter (artikel 5c, se mer om kravet i avsnitt 6.3.7). En avgörande förutsättning för att en privat aktör ska godkännas som tillhandahållare är således att det är fråga om en certifierad identitetsplån bokslösning. Ett sådant villkor i de svenska föreskrifterna medför att granskningen av en anmäld aktör, i detta avseende, främst handlar om att kontrollera att en sådan certifiering är genomförd i enlighet med förordningskraven.

Ett annat väsentligt villkor, som också följer direkt av förordningen, är att det ska vara möjligt att återkalla giltigheten av en europeisk digital identitetsplån bok. Enligt artikel 5a.9 är det medlemsstaterna som ska säkerställa att återkallelse kan ske a) på användarens uttryckliga begäran, b) när den europeiska digitala identitetsplån bokens säkerhet har äventyrats eller c) vid användarens död eller när den juridiska personen upphör med sin verksamhet.

Enligt vår bedömning måste det vara upp till varje aktör som vill godkännas som tillhandahållare av en europeisk digital identitetsplån bok att se till att återkallelse av en plån boksinstans är möjlig enligt artikel 5a.9. Det kan således behöva föreskrivas som ett villkor

för godkännande att tillhandahållaren i angivna fall ska kunna erbjuda tekniska förutsättningar för en återkallelse. Utan att här ange hur villkoren kan utformas noterar vi följande beträffande återkallelse enligt artikel 5a.9 c. I skäl 34 i förordningens ingress anges, som en tänkbar åtgärd, att en mekanism bör inrättas som gör det möjligt för den myndighet som ansvarar för att reglera arvet efter den fysiska personen eller tillgångarna hos den juridiska personen att begära att europeiska digitala identitetsplånböcker omedelbart återkallas i samband med dödsfall eller juridiska personers upphörande.⁷ I Sverige finns ingen myndighet som ansvarar för att reglera arvet efter en fysisk person eller tillgångarna hos en juridisk person, och som i den egenskapen kan begära en återkallelse. Däremot kan sådana privata aktörer som godkänts som tillhandahållare av den europeiska digitala identitetsplånboken erhålla uppgifter om att användare har avlidit respektive upphört med sin verksamhet från befintliga register, såsom Statens personadressregister (SPAR) och skilda register för juridiska personer (se avsnitt 6.3.3). Till skillnad från myndigheter och andra offentliga aktörer är det för privata aktörer förenat med avgifter att få del av sådana uppgifter. Som ett villkor för godkännande kan de svenska föreskrifterna därmed behöva innehålla krav på att tillhandahållaren ska ha åtkomst till relevanta register.

Grunden för återkallelse enligt artikel 5a.9 b är att den europeiska digitala identitetsplånbokens säkerhet har äventyrats. I skäl 34 kommer en grundläggande förutsättning för den europeiska digitala identitetsplånboken till tydligt uttryck, nämligen att det är användarens exklusiva rättighet och val att använda liksom att upphöra att använda identitetsplånboken. Det bör, enligt nämnda skäl, därför utarbetas enkla och säkra förfaranden så att användarna kan begära att giltigheten för europeiska digitala identitetsplånböcker omedelbart återkallas. Utöver tidigare nämnda exempel anges förlust eller stöld, dvs. omständigheter som medför att plånboksinstansens säkerhet är äventyrad. Med hänsyn till innehållet i skäl 34 finns anledning att utgå från att samtliga återkallelsegrunder i artikel 5a.9 tar eller kan ta sikte på plånboksinstanser (se även avsnitt 6.6.3, där bestämmelser om säkerhetsincidenter enligt artikel 5e behandlas).

⁷ En annan möjlighet skulle kunna vara att tillhandahållaren av uppgifter för personidentifiering (PID) direkt av tillhandahållaren av identitetsplånboken begär att den ska återkallas, se The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework Architecture and Reference Framework version 1.4.0, avsnitt 6.5.4.

Centralt för den europeiska digitala identitetsplån-boken är att dess kostnadsfria anskaffning, användning och återkallande i fråga om fysiska personer och att all behandling av personuppgifter ska utföras i enlighet med EU:s dataskyddsförordning. Vidare ska sådana identitetsplån-böcker göras tillgängliga för användning av personer med funktionsnedsättning på samma villkor som andra användare. Det är således villkor som måste uppfyllas för ett godkännande och garanteras av tillhandahållaren.

Exempel på ytterligare villkor för godkännande, som det kan finnas anledning att föreskriva om, är säkerställandet av att det finns förutsättningar för validering av tillhandahållna identitetsplån-böcker. Det är ännu oklart vilka tekniska lösningar som kommer att användas för validering, eftersom detta ska regleras genom kommande genomförandeakter. Ett godkännande kan dock behöva villkoras av att tillhandahållaren ska tillse att den europeiska digitala identitetsplån-boken omfattas av en förteckning så att de plån-boksinstanser som används kan valideras (se mer om valideringsmekanismer i avsnitten 4.7.4 och 6.3.6).

Vid sidan av de skyldigheter som följer direkt av den reviderade eIDAS-förordningen kan det finnas anledning att också uppställa vissa krav på aktören, avseende bl.a. associationsform, organisation och etablering. Utan att ta ställning till vilka som bör kunna komma i fråga för ett godkännande får det anses vara lämpligt att enbart associationer med grundreglering som innebär viss garanti när det gäller varaktighet, kapitalinsats, tillfredsställande revision etc. bör accepteras för att allmänhetens intressen ska kunna anses vara tillvaratagna.⁸ Aktören ska t.ex. förfoga över tillräckliga medel för att bedriva verksamheten under överskådlig tid och ha förmåga att bära risken för skadeståndsskyldighet. Aktören bör vidare vara etablerad i Sverige.

Vidare bör uppställas krav på ledningssystem för informations-säkerhet och nödvändiga operationella krav på tillhandahållarens verksamhet avseende bl.a. systematisk riskhantering och internkontroll respektive personalsäkerhet.⁹ Det handlar således om sådana förutsättningar som inte omfattas av krav enligt föreskrivna certifieringsordningar (se avsnitt 6.3.7).

⁸ Sådana krav förekommer bl.a. för tillståndspliktiga aktörer på finansmarknadsområdet, se t.ex. prop. 2002/03:139 s. 402.

⁹ Ytterligare vägledning för dessa krav kan hämtas i Diggs tillitsramverk för Svenska e-legitimationer, se www.digg.se/digitala-tjanster/e-legitimering/tillitsnivaer-for-e-legitimering/tillitsramverk-for-svensk-e-legitimation (hämtad 2024-05-27).

Myndigheten för digital förvaltning är lämpad att tillhandahålla den europeiska digitala identitetsplånboken

Digg ska enligt sin myndighetsinstruktion samordna och stödja den förvaltningsgemensamma digitaliseringen i syfte att göra den offentliga förvaltningen mer effektiv och ändamålsenlig.¹⁰ Med den offentliga förvaltningen avses kommuner och regioner samt statliga myndigheter med vissa undantag. Inom ansvarsområdet ligger bl.a. att ansvara för den förvaltningsgemensamma digitala infrastrukturen.

Vidare har myndigheten enligt sin instruktion ett flertal uppgifter med anknytning eller direkt hänvisning till eIDAS-förordningen, såsom ansvaret för den offentliga förvaltningens tillgång till infrastruktur och tjänster för elektronisk identifiering och underskrift, inbegripet ansvaret för de svenska förbindelsepunkterna (noderna) för gränsöverskridande elektronisk identifiering i enlighet med eIDAS-förordningen. Myndigheten ska också uppfylla de samarbetskyldigheter som gäller för Sverige som medlemsstat enligt förordningen och vara gemensam kontaktpunkt för samarbetet, företräda Sverige i övriga frågor som rör gränsöverskridande elektronisk identifiering enligt förordningen samt lämna stöd och information till myndigheter i sådana frågor.

Diggs nuvarande uppdrag och ansvar faller således väl in under den reviderade eIDAS-förordningens utökade tillämpningsområde avseende den europeiska digitala identitetsplånboken.

Andra offentliga aktörer som skulle kunna ansvara för uppgiften och som övervägts av utredningen är Polismyndigheten och Skatteverket, vilka ansvarar för utfärdande av det nationella identitetskortet respektive identitetskort för folkbokförda i Sverige.¹¹ Hos båda myndigheter finns nödvändig kunskap och erfarenhet av grundidentifiering av den som ansöker om identitetshandlingar och därmed sammanhörande ärendehandläggning.¹²

Den europeiska digitala identitetsplånboken är i och för sig ett medel för elektronisk identifiering. Tillhandahållandet av en sådan

¹⁰ Förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning.

¹¹ Se förordningen (2005:661) om nationellt identitetskort och lagen (2015:899) om identitetskort för folkbokförda i Sverige.

¹² För innebörden av begreppet grundidentifiering, se t.ex. delbetänkandet *En säker och tillgänglig statlig e-legitimation* (SOU 2023:61), s. 160 ff.

identitetsplånbok påminner dock mer om en form av id-växling.¹³ Det krävs, som vi återkommer till nedan, en e-legitimation på tillitsnivå hög för tillgång till och ibruktagande av ("onboarding") en europeisk digital identitetsplånbok. Grundidentifieringen av användaren är därmed redan gjord.

Den primära uppgiften för den myndighet som ska ansvara för att tillhandahålla den europeiska digitala identitetsplånboken är således att ta fram och förvalta en sådan identitetsplånbok, som ska tillhandahållas inom ramen för ett system för elektronisk identifiering.

I skäl 29 anges att syftet med den reviderade förordningen är att förse användaren med "en helt mobil, säker och användarvänlig europeisk digital identitetsplånbok". Det är tillhandahållarna av identitetsplånboken som ansvarar för att se till att kraven för denna är uppfyllda.¹⁴ Det är således fråga om en, i mångt och mycket, teknikintensiv uppgift. Utvecklingen inom ifrågavarande område bör bedrivas sammanhållet av en myndighet. På så sätt kan kompetens byggas upp och stärkas samt frågorna få den kontinuitet som krävs. Mot denna bakgrund framstår Digg som mest lämpad för uppgiften att tillhandahålla den europeiska digitala identitetsplånboken.

Att en offentlig aktör åläggs detta ansvar innebär dock inte en skyldighet att inom den egna organisationen utveckla och ta fram en sådan identitetsplånbok med den bakomliggande infrastruktur som är nödvändig, eller att hantera alla andra aspekter av den löpande förvaltningen såsom användarsupport. Den ansvariga aktören kan upphandla själva handhavandet av den digitala identitetsplånboken från en eller flera leverantörer.

Förslaget att en statlig myndighet utses för att tillhandahålla den europeiska digitala identitetsplånboken är, som framgått, avsett att garantera att Sverige ska kunna uppfylla kraven i den reviderade eIDAS-förordningen inom föreskriven tidsram och över tid. Samtidigt möjliggör vårt förslag att även privata aktörer ska ges möjlighet att erbjuda sådana identitetsplånböcker. Digg kommer enligt vårt förslag i så fall att granska och godkänna sådana aktörer, i viss utsträckning mot villkor i föreskrifter som myndigheten själv kan komma att

¹³ Begreppet id-växling brukar användas när en e-legitimation, som utfärdas efter en grundidentifiering, kan utgöra underlag vid utfärdande av andra e-legitimationer, se t.ex. betänkanudet *Ett säkert ID-kort – med e-legitimation* (SOU 2019:14), s. 321.

¹⁴ The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework, The European Digital Identity Wallet Architecture and Reference Framework, ver. 1.4.0, avsnitt 3.2.

meddela. Det blir dock inte fråga om en sådan situation med dubbla roller som förslaget om en statligt tillhandahållen e-legitimation innebär.¹⁵ En godkänd tillhandahållare av den europeiska digitala identitetsplån-boken kommer, i likhet med Digg, att stå under tillsyn. Om det finns anledning att anta att villkoren för godkännandet av den privata aktören inte längre är uppfyllda ska Digg underrätta tillsynsmyndigheten om detta och inte vidta några ytterligare åtgärder. Det är inte aktuellt för Digg att pröva sin verksamhet med den digitala identitetsplån-boken mot egna uppställda krav, utan myndigheten har att efterleva de skyldigheter som följer direkt av den reviderade eIDAS-förordningen och dess kommande genomförandeakter.

Användningen av den europeiska digitala identitetsplån-boken förutsätter, som redan angetts, att tillhandahållna plån-boksinstanser kan valideras. Som behandlas närmare i det följande får det anses vara naturligt att det åvilar tillhandahållaren av en sådan identitetsplån-bok att göra information tillgänglig för validering (se vidare avsnitt 6.3.6)

Enligt artikel 5d.1 ska medlemsstaterna utan onödigt dröjsmål informera kommissionen och samarbetsgruppen enligt artikel 46e.1 om europeiska digitala identitetsplån-böcker som har certifierats och tillhandahållits. Medlemsstaterna ska utan onödigt dröjsmål också informera kommissionen och samarbetsgruppen om en certifiering upphör att gälla och ange skälen till detta. Vad informationen närmare ska innefatta framgår av artikel 5d.2. Det handlar om bl.a. om uppgifter om certifikatet och rapporten om certifieringsbedömningen för den tillhandahållna identitetsplån-boken, en beskrivning av det system för elektronisk identifiering inom ramen för vilket den europeiska digitala identitetsplån-boken tillhandahålls och system för tillfälligt upphävande eller återkallande av det anmälda systemet för elektronisk identifiering eller autentisering eller av de berörda äventyrade delarna. Enligt vår uppfattning får det anses naturligt att detta är en del i ansvaret för den tillhandahållande myndigheten. Ansvaret omfattar även information om sådana europeiska digitala identitetsplån-böcker som erbjuds av privata aktörer som efter granskning har godkänts som tillhandahållare.

¹⁵ *En säker och tillgänglig statlig e-legitimation* (SOU 2023:61), s. 182 ff. och 207 f.

En identitetsplånbok för både fysiska och juridiska personer

Den europeiska digitala identitetsplånboken ska, som nämnts, tillhandahållas inom ramen för ett system för elektronisk identifiering. Detta framgår av artikel 5d.2 b och det följer även av bl.a. artikel 5a.5 f. I punkten 11 i sistnämnda artikel preciseras att det ska vara fråga om ett system för elektronisk identifiering med tillitsnivå hög.

Det är först när uppgifter för personidentifiering (PID) kopplats till en plånboksinstans som användaren har en giltig europeisk digital identitetsplånbok (se avsnitten 4.7 och 6.3.3). Kopplingen kommer att förutsätta en e-legitimation på tillitsnivå hög. Detta följer av artikel 5a.24. Av artikeln framgår förvisso att även en e-legitimation på tillitsnivå väsentlig kan komma att vara tillräcklig för anslutning och ibruktagande ("onboarding") av den europeiska digitala identitetsplånboken. Det förutsätter dock att e-legitimationen kombineras med sådana ytterligare förfaranden för distansanslutning i säkerhets-höjande syfte och som, i förening med e-legitimationen, medför att kraven för tillitsnivå hög är uppfyllda. Reglering om detta ska fastställas i genomförandeakter av kommissionen (artikel 5a.24).

För närvarande finns det ingen e-legitimation på tillitsnivå hög i Sverige för allmänheten. Digg har i år fått i uppdrag att utveckla en sådan.¹⁶ Enligt det förslag som lämnades i vårt delbetänkande ska en statlig e-legitimation på tillitsnivå hög tillhandahållas den som har svenskt personnummer, alternativt samordningsnummer för personer med styrkt identitet vilket inte är vilandeförklarat. Det föreslogs också en minimiålder om nio år.¹⁷ Förslaget bereds i Regeringskansliet. Det är därmed oklart vilka villkor som kommer att gälla för att tillhandahållas den statliga e-legitimationen som ska utvecklas av Digg.

Vem som kan anskaffa en europeisk digital identitetsplånbok kan sägas bero på vem som kan tillhandahållas en e-legitimation på tillitsnivå hög (alternativt tillitsnivå väsentlig i kombination med säkerhets-höjande åtgärder). Av artikel 5a.1 följer att alla fysiska och juridiska personer ska tillhandahållas den europeiska digitala identitetsplånboken. Att i svensk författning precisera kretsen närmare är med

¹⁶ Regleringsbrev för budgetåret 2024 avseende Myndigheten för digital förvaltning, 2023-12-21 Fi2023/00936 och Fi2023/03265 (delvis).

¹⁷ *En säker och tillgänglig statlig e-legitimation* (SOU 2023:61) s. 145 ff. Förslag om en statlig e-legitimation har lämnats också i betänkandena *reboot – en omstart för den digitala förvaltningen* (SOU 2017:114) och *Ett säkert statlig ID-kort – med e-legitimation* (SOU 2019:14).

beaktande av det anförda inte lämpligt. I avsnitt 6.3.3 återkommer vi till detta och även juridiska personers anskaffning av en identitetsplånbok, eller organisationsplånbok, som det – i särskiljande syfte – ibland också benämns.

Av den reviderade eIDAS-förordningen följer, som framgått, att en användare av den europeiska digitala identitetsplånboken ska kunna interagera inte bara med förlitande parter utan också att sådana identitetsplånböcker ska kunna interagera sinsemellan i syfte att bl.a. ta emot, validera och dela uppgifter för personidentifiering och elektroniska attributsintyg på ett säkert sätt (artikel 5a.5 vi).

För att också företag och andra organisationer ska kunna arbeta med sådana utbyten i automatiserade flöden sinsemellan, behövs en europeisk digital identitetsplånbok utvecklad specifikt för juridiska personer.

Parallellt med arbetet att ta fram den europeiska digitala identitetsplånboken för fysiska personer måste således en för juridiska personer anpassad variant utarbetas. Det finns inte anledning att en sådan organisationsplånbok tillhandahålls av en annan myndighet än den som tillhandahåller den europeiska digitala identitetsplånboken för fysiska personer. Det är däremot av vikt att utvecklingsarbetet sker i nära samråd och samarbete med Bolagsverket och övriga för området relevanta myndigheter och organisationer, såsom Tillväxtverket och Sveriges Kommuner och Regioner (SKR).

Avgiftsuttag för att tillhandahålla den europeiska digitala identitetsplånboken till juridiska personer

Som redovisats inledningsvis (avsnitt 4.7.1) ska utfärdandet, användningen och återkallandet av europeiska digitala identitetsplånböcker vara utan kostnad för fysiska personer (se artikel 5a.13). Motsvarande begränsning finns enligt den reviderade eIDAS-förordningen inte för juridiska personer som vill ansöka om en europeisk digital identitetsplånbok, en s.k. organisationsplånbok.

Anskaffandet av en organisationsplånbok syftar till att tillgodose den enskilda organisationens behov. Även om full kostnadstäckning inte kommer att uppnås är det naturligt att tillhandahållandet finansieras av användarna genom avgifter (se, för motsvarande bedömning avseende tillhandahållande av personidentifieringsuppgifter till organisationsplånboken, avsnitt 6.3.3). Regeringen, eller efter regeringens

bemyndigande, den myndighet som tillhandahåller den europeiska digitala identitetsplån boken för juridiska personer ska därför ges möjlighet att införa ett avgiftssystem. Närmare bestämmelser om avgiftssystemets utformning kan meddelas med stöd av föreslaget bemyndigande som tas in i kompletteringslagen.

6.3.2 Den tillhandahållande myndigheten får meddela vissa ytterligare föreskrifter

Utredningens förslag: Den myndighet som utsetts att tillhandahålla den europeiska digitala identitetsplån boken får meddela föreskrifter om:

- ytterligare funktioner för den europeiska digitala identitetsplån boken, inbegripet interoperabilitet med befintliga nationella medel för elektronisk identifiering (artikel 5a.7 i EU:s reviderade förordning om elektronisk identifiering) och
- undantag från krav att tillhandahålla öppen källkod (artikel 5a.3 i nämnda förordning).

Utredningens bedömning: Det finns för närvarande inte behov av att meddela föreskrifter om åtgärder för att säkerställa att fysiska personers kostnadsfria användning av kvalificerade elektroniska underskrifter är begränsad till icke-yrkesmässiga ändamål (artikel 5a.5 andra stycket).

Skälen för utredningens förslag och bedömning

Det finns behov av ytterligare föreskriftsbemyndiganden

Den reviderade eIDAS-förordningen innehåller krav som enligt vår bedömning inte för närvarande, men i framtiden kan komma att kräva ytterligare föreskrifter. Den tillhandahållande myndigheten ska därför få meddela föreskrifter för att reglera eventuella ytterligare funktioner för de europeiska digitala identitetsplån böckerna, inbegripet interoperabilitet med befintliga nationella medel för elektronisk identifiering (artikel 5a.7) och om undantag från krav på att tillhandahålla öppen källkod (artikel 5a.3). Föreskrifter om sådana undantag får gälla

källkod för bibliotek, kommunikationskanaler eller andra element som inte finns på användarenheten, förutsatt att det finns skäl med hänsyn till den allmänna säkerheten, se skäl 33 i ingressen till den reviderade eIDAS-förordningen.

Det saknas behov av att begränsa fysiska personers kostnadsfria användning av kvalificerade elektroniska underskrifter

Förordningen tillåter att medlemsstaterna föreskriver proportionella åtgärder för att säkerställa att fysiska personers kostnadsfria användning av kvalificerade elektroniska underskrifter är begränsad till icke-yrkesmässiga ändamål (artikel 5a.5 andra stycket). Enligt vår bedömning skulle ett sådant behov kunna aktualiseras vid användning av den europeiska digitala identitetsplånboken inom ramen för enskild näringsverksamhet, för vilken organisationsnumret motsvaras av personnumret för en fysisk person. Vi bedömer emellertid att den ekonomiska nyttan en sådan föreskrift skulle medföra är försumbar i förhållande till de kostnader som ett system för att särskilja användningen skulle innebära. Av det skälet bedömer vi att det för närvarande inte finns behov av att meddela några sådana föreskrifter.

6.3.3 Tillhandahållare av uppgifter för personidentifiering

Utredningens förslag: De statliga myndigheter som regeringen bestämmer ska tillhandahålla elektroniska attesteringar av sådana uppgifter för personidentifiering för fysiska och juridiska personer (PID respektive LPID) som förutsätts för att en europeisk digital identitetsplånbok ska kunna användas som medel för elektronisk identifiering.

För tillhandahållande av uppgifter för personidentifiering till juridiska personer får en avgift tas ut av den myndighet som tillhandahåller sådana uppgifter.

Utredningens bedömning: Myndigheten för digital förvaltning, Polismyndigheten och Skatteverket är, var för sig, lämpade att tillhandahålla PID avseende fysiska personer. Effektivitetsskäl talar för att uppgiften bör utföras av Myndigheten för digital förvaltning.

Bolagsverket, Skatteverket och Statistiska centralbyrån är, var för sig, lämpade att tillhandahålla LPID för juridiska personer. Effektivitetsskäl talar för ett sammanhållet ansvar hos en myndighet och att uppgiften bör utföras av Bolagsverket.

Skälen för utredningens förslag och bedömning

Inledning

En förutsättning för användning av den europeiska digitala identitetsplånboken som medel för identifiering och för bl.a. lagring av elektroniska attributsintyg är, som tidigare konstaterats, att den först förses med uppgifter för personidentifiering relaterade till en fysisk eller juridisk person, dvs. det som i detta sammanhang även benämns PID ("personal identification data"). Enligt artikel 3.3 definieras uppgifter för personidentifiering som:

en uppsättning uppgifter som utfärdas i enlighet med unionsrätten eller nationell rätt, som gör det möjligt att fastställa identiteten på en fysisk eller juridisk person eller på en fysisk person som företräder en annan fysisk person eller en juridisk person

För att särskilja PID för fysiska personer från PID för juridiska personer förekommer även förkortningen LPID ("legal PID"). Om inte särskilt anges i det följande omfattar PID, i förekommande fall, även LPID.

I skäl 19 till den reviderade eIDAS-förordningen anges att det endast är medlemsstaternas behöriga myndigheter som kan fastställa identiteter med en hög tillförlitlighetsnivå och därmed garantera att en person faktiskt är den som han eller hon påstår sig vara. Av den anledningen måste tillhandahållandet av de europeiska digitala identitetsplånböckerna bygga på den juridiska identiteten för unionsmedborgare, invånare i unionen eller juridiska personer.

Genom att europeiska digitala identitetsplånböcker förses med utfärdade PID är det, på ett tekniskt tillförlitligt sätt, möjligt att elektroniskt visa att den som förfogar däröver har en identitet som är registrerad i en befolkningsdatabas. Utfärdade PID är en attesting

i elektronisk form.¹⁸ Med andra ord utgör PID bestyrkta och tekniskt kontrollerbara uppgifter om att en person har en i en medlemsstat registrerad identitet som fortfarande är i kraft.

Detta kräver dock att det inte får finnas två personer med samma uppgiftsuppsättning avseende obligatoriska attribut, och att dessa utgörs av åtminstone minimiuppsättningen enligt kommissionens genomförandeförordning CIR 2015/1501.¹⁹

I den reviderade eIDAS-förordningen används inte uttrycket ”tillhandahållare” i anslutning till ”uppgifter för personidentifiering”. I stället föreskrivs i artikel 5a.18 att medlemsstaterna ska informera kommissionen om ”de organ som ansvarar för att säkerställa att uppgifter för personidentifiering är kopplade till den europeiska digitala identitetsplånboken i enlighet med artikel 5a.5 f”. Av sistnämnda artikel följer att ifrågavarande uppgifter är sådana som är ”tillgängliga från det system för elektronisk identifiering under vilket den europeiska digitala identitetsplånboken tillhandahålls”. Det ansvariga organet ska alltså säkerställa att dessa uppgifter på ett unikt sätt avser personen i fråga och är kopplade till identitetsplånboken.

Däremot används benämningen tillhandahållare av PID i den s.k. ARF:en (se avsnitt 4.7.2). Där anges att tillhandahållare av PID är betrodda enheter (”trusted entities”) som ansvarar för att:

- verifiera identiteten hos en användare av den digitala identitetsplånboken i enlighet med kraven för tillitsnivå hög,
- utfärda PID till den digitala identitetsplånboken i ett harmoniserat gemensamt format, och
- göra information tillgänglig för förlitande parter för att möjliggöra validering av PID.²⁰

¹⁸ The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework, The European Digital Identity Wallet Architecture and Reference Framework, ver. 1.4.0, avsnitt 5.1.

¹⁹ Kommissionens genomförandeförordning (EU) 2015/1501 av den 8 september 2015 om interoperabilitetsramverket enligt artikel 12.8 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden. Genom kommande genomförandeakter kan antas att den obligatoriska uppgiftsuppsättningen kommer att få kompletteras med ytterligare, frivilliga, attribut.

²⁰ Villkoren för dessa tjänster ska fastställas av varje medlemsstat, se The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework, The European Digital Identity Wallet Architecture and Reference Framework, ver. 1.4.0, avsnitt 3.3.

Verifiering av identiteten hos användaren, som innebär att det görs kontroller av bl.a. att attribut stämmer med schema och att utfärdaren är utgivare av schemat, är således en grundförutsättning för anslutning och ett ibruktagande av en identitetsplånboksinstans ("onboarding"). Som konstateras i avsnitten 4.7 och 6.3.1 krävs för koppling av PID till en identitetsplånboksinstans att användaren har en e-legitimation med tillitsnivå hög, eller med tillitsnivå väsentlig i förening med sådana säkerhetshöjande åtgärder som avses att regleras i kommande genomförandeakter enligt artikel 5a.24. Grundidentifieringen av användaren är således redan gjord.

Utöver fysiska personer avses med användare bl.a. en juridisk person eller en fysisk person som företräder en juridisk person (se definitionen i artikel 3.5a). Vem som i praktiken kan vara en användare beror på medlemsstaternas nationella lagstiftning. Det finns inget i svensk lagstiftning som hindrar en juridisk person från att vara en användare i den reviderade eIDAS-förordningens mening.

Till skillnad mot fysiska personer kan dock juridiska personer i Sverige inte identifiera sig elektroniskt (eller analogt). Att kontrollera identiteten hos en användare av en europeisk digital identitetsplånbok i samband med anslutning och ibruktagande ("onboarding") får, i fråga om en juridisk person, förstås som att det är dess behöriga representants eller företrädares identitet som kontrolleras.

Validering är en process genom vilken det kontrolleras och bekräftas att data i elektronisk form är giltiga i enlighet med förordningen (se definition i artikel 3.41). Av artikel 5b.9 framgår att förlitande parter "ska ansvara för genomförandet av förfarandet för autentisering och validering av uppgifter för personidentifiering och elektroniska attributsintyg som begärts från en europeisk digital identitetsplånbok". På tillhandahållaren av PID åvilar därmed att göra information tillgänglig för förlitande parter för att möjliggöra validering av PID. Ogiltighet föranleds av att giltighetstiden löpt ut eller att tillhandahållaren återkallat utfärdade PID (se avsnitt 4.7.5).

Återkallelse av PID, tillika tillgängliggörande av information för validering, förutsätter att tillhandahållaren har uppdaterad information om utfärdade PID. I skrivande stund råder oklarhet om vilken eller vilka tekniska lösningar som kommer att bli aktuella för att skapa tillit i ekosystemet för den europeiska digitala identitetsplånboken. I våra överväganden har vi utgått från att tillhandahållare av PID därför behöver ha en förteckning eller en lösning liknande den tillits-

förteckning som möjliggör validering av kvalificerade betrodda tjänster (se mer om detta i avsnitt 6.3.6).

Vilken eller vilka myndigheter är lämpade för uppgiften att tillhandahålla PID för koppling till en europeisk digital identitetsplånbok för fysiska personer?

Den eller de aktörer som utfärdar eller tillhandahåller t.ex. officiella fysiska identitetshandlingar, e-legitimationer, eller den europeiska digitala identitetsplånboken kan vara tillhandahållare av PID. Tillhandahållare av den europeiska digitala identitetsplånboken får alltså (men behöver inte) vara samma aktör som tillhandahåller PID. Om det är en och samma aktör ska den dock uppfylla samtliga krav för såväl tillhandahållare av PID som tillhandahållare av den europeiska identitetsplånboken.²¹

Nödvändiga uppgifter för tillhandahållande av PID för fysiska personer finns i folkbokföringsdatabasen som Skatteverket ansvarar för. Myndigheten utfärdar även identitetshandlingar enligt lagen om identitetskort för folkbokförda i Sverige, och har därmed förutsättningar att utföra denna uppgift. Detsamma gäller Polismyndigheten som, utöver pass, utfärdar det nationella identitetskortet enligt förordningen om nationellt identitetskort, och har därigenom egen tillgång till uppgifter för personidentifiering för fysiska personer.

Givet att lämnat förslag om statlig e-legitimation genomförs och Digg utses till utfärdare kan det vara möjligt att samhantera utfärdande av den statliga e-legitimationen och tillhandahållande av PID för fysiska personer.²² Digg har, i sådant fall, i egenskap av ansvarig för den föreslagna databasen över statliga e-legitimationer tillgång till nödvändiga uppgifter för att tillhandahålla PID för fysiska personer. Om förslaget om den statliga e-legitimationen inte genomförs kan Digg enligt 2 kap. 8 § första stycket lagen (2001:182) om behandling av personuppgifter i Skatteverkets folkbokföringsverksamhet medges direktåtkomst till uppgift om bl.a. person- och samordningsnummer, namn, adress och avregistrering från folkbokföringen.²³ Det

²¹ The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework, The European Digital Identity Wallet Architecture and Reference Framework, ver. 1.4.0, avsnitt 3.3.

²² *En säker och tillgänglig statlig e-legitimation* (SOU 2023:61) s. 180 ff.

²³ Se prop. 2020/21:160 s. 16 f.

bedöms därmed inte finnas något sekretesshinder för överföring av nödvändiga uppgifter för tillhandahållandet av PID.

Möjligheten att samhantera tillhandahållande av PID för fysiska personer med tillhandahållandet av själva identitetsplånboken talar för att det bör vara en och samma myndighet som ansvarar för uppgifterna. Mot bakgrund av vår bedömning i föregående avsnitt är det således mest lämpligt att Digg ges i uppdrag att tillhandahålla PID för fysiska personer.

Vilken eller vilka myndigheter är lämpade för uppgiften att tillhandahålla PID för koppling till en europeisk digital identitetsplånbok för juridiska personer?

När det gäller uppgifter för personidentifiering för juridiska personer råder delvis andra förutsättningar, inte minst den omständigheten att det handlar om flera olika kategorier av associationer.

Enligt gällande interoperabilitetsramverk utgörs de obligatoriska personidentifieringsuppgifterna för juridiska personer av ”nuvarande juridiska namn” och ”en unik identitetsbeteckning som satts samman av den utsändande medlemsstaten i enlighet med de tekniska specifikationerna för gränsöverskridande identifiering och som är mest beständig i tid”.²⁴

Organisationsnummer är den identitetsbeteckning som i Sverige tilldelas juridiska personer, exempelvis företag och ideella organisationer. Ett tilldelat organisationsnummer får inte ändras eller användas på nytt vid tilldelning av nummer (4 § lagen [1974:174] om identitetsbeteckning för juridiska personer m.fl.). Det innebär att ett organisationsnummer är evigt och unikt.²⁵ Som sådant omfattas därmed organisationsnummer av definitionen av uppgifter för personidentifiering för juridiska personer i eIDAS-förordningen och interoperabilitetsramverket.

²⁴ Kommissionens genomförandeförordning (EU) 2015/1501 av den 8 september 2015 om interoperabilitetsramverket enligt artikel 12.8 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden. Minimiuppsättningen av uppgifter för juridiska personer finns i bilagan till genomförandeförordningen.

²⁵ En juridisk person behåller ett tilldelat nummer under hela sin livstid och numret får aldrig tilldelas någon annan juridisk person (prop. 1974:56 s. 19). I vissa fall kan ett organisationsnummer återaktiveras i organisationsnummerregistret. För svenska juridiska personer prövas återaktivering av ett organisationsnummer utifrån bestämmelserna i förvaltningslagen (2017:900).

Alla juridiska personer har dock inte ett organisationsnummer. I 1 § nyss nämnda lag anges vilka organisationer som *ska* ha ett organisationsnummer:

1. aktiebolag, europabolag och europakooperativ med säte i Sverige, handelsbolag, ekonomiska föreningar och samfällighetsföreningar, ömsesidiga försäkringsbolag, ömsesidiga tjänstepensionsbolag, försäkringsföreningar och tjänstepensionsföreningar,
2. erkända arbetslöshetskassor och andra inrättningar som enligt lag eller annan författning står under offentlig tillsyn,
3. kommuner, regioner, kommunalförbund och andra organ för samverkan mellan kommuner,
4. registrerade trossamfund och deras organisatoriska delar, och
5. stiftelser.

Även andra juridiska personer ska tilldelas organisationsnummer, t.ex. ideella föreningar, om den juridiska personen eller en statlig myndighet begär det. Detta gäller även enkla bolag, partrederier och utländska företags filialer i Sverige (2 §). Därutöver får statliga myndigheter tilldelas organisationsnummer (3 §).

Till skillnad från personnummer och samordningsnummer tilldelas organisationsnummer inte heller av en och samma aktör utan av den myndighet som registrerar den juridiska personen när den bildas eller när det annars finns anledning att föra in organisationen i myndighetens register. De som främst hanterar tilldelning av organisationsnummer är Bolagsverket (för t.ex. aktiebolag), Skatteverket (för t.ex. stiftelser och ideella föreningar) och Statistiska centralbyrån (för t.ex. kommuner samt statliga och regionala myndigheter). De övriga myndigheterna är Kammarkollegiet, Lantmäteriet, Länsstyrelsen och Inspektionen för arbetslöshetsförsäkringen.²⁶

Skatteverket har tillsynen över tilldelningen av organisationsnummer och för också ett centralt register över tilldelade organisationsnummer i hela landet (5 §). Utöver organisationsnummer finns i registret uppgift om namn, adress, geografiska koder för säte (län och kommun), kod för juridisk form, markering i förekommande fall för konkurs och likvidation, tidpunkt för registrering och even-

²⁶ www4.skatteverket.se/rattsligvagledning/edition/2024.1/1725.html (hämtad 2024-05-27).

tuell avregistrering i organisationsnummerregistret. Efter registrering i organisationsnummerregistret får alla registrerade ett meddelande om tilldelat organisationsnummer. Även vid inaktivering sänds ett meddelande ut. Flera myndigheter får automatiskt uppgift om insättning, ändring och avregistrering av organisationsnummer.²⁷ Det har inte framkommit något behov av författningsreglering för en sådan uppgiftsöverföring.

Vid sidan av Skatteverkets register över organisationsnummer finns även ett allmänt företagsregister.²⁸ Det är Statistiska centralbyrån som ansvarar för detta register enligt förordningen (1984:692) om det allmänna företagsregistret. Registret omfattar uppgifter om bl.a. de associationer som har tilldelats organisationsnummer enligt lagen om identitetsbeteckning för juridiska personer m.fl., enskilda näringsidkare som har förts in i ett handelsregister, fysiska personer och dödsbon som regelbundet bedriver näringsverksamhet eller som regelbundet har någon anställd (2 §). Eftersom registret omfattar alla som har tilldelats organisationsnummer ingår uppgifter även för exempelvis kommuner och myndigheter (som här också går under benämningen företag). Registret innehåller en mängd ytterligare uppgifter relaterade till de registrerade företagen än Skatteverkets organisationsnummerregister (6–9 §§).

Det allmänna företagsregistret uppdateras kontinuerligt med uppgifter från främst Skatteverket och Bolagsverket, men även genom Statistiska centralbyråns egna utredningar (19 §). Såväl myndigheter som enskilda får använda registret (5 §). Utlämnande av uppgifter sker i form av utskrift, på medium för automatisk databehandling eller genom att en eller flera terminaler eller datorer ansluts till registret (16 §).

Även Bolagsverket har ansvar att bl.a. tillhandahålla effektiva och ändamålsenliga system för registreringsärenden. I verkets uppdrag ingår ett ansvar att registrera t.ex. företag och föreningar. Ansvaret är dock, som framgått, avgränsat till särskilt angivna associationer. Det rör sig exempelvis om banker, Europabolag, försäkrings- och tjänstepensionsföretag, samt övriga aktiebolag respektive ekonomiska för-

²⁷ www.skatteverket.se/foretag/drivaforetag/startaochregistrera/organisationsnummer.4.361dc8c15312eff6fd235d1.html?q=register+organisationsnummer (hämtad 2026-05-27).

²⁸ Registret är urvalsram för statistiska undersökningar och ger underlag för sammanställningar av uppgifter om företag och arbetsställen i Sverige. Uppgifterna i registret kan dessutom nyttjas av andra för att komplettera och kontrollera uppgifter i andra register samt komplettera och kontrollera uppgifter i övrigt om de fysiska och juridiska personer som omfattas av registret (4 § förordningen om det allmänna företagsregistret).

eningar, Europakollektiv, samt filialer (dvs. ett utländskt företag som bedriver näringsverksamhet i Sverige genom ett avdelningskontor med självständig förvaltning).²⁹

Varken det centrala registret över organisationsnummer, det allmänna företagsregistret, eller Bolagsverkets register innehåller således uppgifter om *samtliga* juridiska personer som enligt den reviderade eIDAS-förordningen ska kunna tillhandahållas en sådan identitetsplånbok (härefter organisationsplånbok). De juridiska personer för vilka organisationsnummer inte är ett författningsreglerat krav kommer alltså att behöva begära att tilldelas ett sådant av ansvarig myndighet. Först när organisationsnummer är registrerat finns förutsättning för att en organisationsplånbok ska kunna tillhandahållas.

Vad gäller kravet på kontroll av användarens identitet får, som tidigare anförts, det förstås på så vis att det är identiteten hos den juridiska personens behöriga representant eller företrädare som avses.

Som framgått innehåller registret över organisationsnummer och det allmänna företagsregistret, till skillnad från Bolagsverkets register, inte uppgifter om behöriga företrädare. I nuläget går det således inte att, vid anslutning till organisationsplånboken och via densamma, åstadkomma en automatiserad process för kontroll av behöriga företrädares identitet mot uppgifter i befintliga register, utan annan hantering kommer att krävas beträffande vissa juridiska personer och deras företrädare.

Det ligger inte inom ramen för utredningens uppdrag att se över vare sig förutsättningarna för att samla ansvaret för registrering av samtliga juridiska personer hos en och samma myndighet eller innehållet i förda register.

Oberoende av rådande omständigheter får det, av kostnads- och effektivitetsskäl, anses vara motiverat att hos en myndighet samla ansvaret att tillhandahålla LPID för den europeiska digitala identitetsplånboken. I lagen med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering ska därför införas en bestämmelse som bemyndigar regeringen att utse den myndighet som för juridiska personer ska tillhandahålla sådana uppgifter för personidentifiering som avses i artikel 3 i EU:s förordning om elektronisk identifiering, och som ska kunna kopplas till den europeiska digitala identitetsplånboken.

²⁹ <https://bolagsverket.se/omoss/varverksamhet/vadviregistrerar.2069.html> (hämtad 2024-05-27).

Samtliga här redovisade myndigheter är lämpade för en sådan uppgift. De har eller kan medges tillgång till erforderliga uppgifter för tillhandahållande av LPID, såsom organisationsnummer, i de register som redan förs av respektive myndighet genom elektroniskt utlämnande, t.ex. direktåtkomst.³⁰ Något sekretesshinder bedöms inte föreligga för överföring av nödvändiga uppgifter för tillhandahållandet av LPID.

Bolagsverkets ansvar omfattar visserligen inte samtliga juridiska personer som ska kunna tillhandahållas en europeisk digital identitetsplånbok, men likväl lejonparten av associationer som kan förväntas anskaffa en sådan organisationsplånbok. Nuvarande ansvarsområden och den omständigheten att Bolagsverket, tillsammans med finska staten, leder ett av de tidigare nämnda storskaliga pilotprojekten avseende den europeiska digitala identitetsplånboken³¹ gör verket rustat för uppgiften att tillhandahålla uppgifter för personidentifiering för den europeiska digitala identitetsplånboken för juridiska personer. Vi bedömer därför det lämpligt att Bolagsverket ansvarar för denna uppgift.

Beträffande enskilda näringsidkare har, vid utredningens kontakter med Bolagsverket, anförts att dessa inte torde kunna omfattas av den kategori aktörer som kan tillhandahållas en organisationsplånbok, dvs. europeisk digital identitetsplånbok för juridiska personer, eftersom en enskild näringsidkare enligt svensk rätt inte omfattas av begreppet juridisk person. En enskild näringsidkare kan således inte tilldelas ett organisationsnummer vilket, som tidigare anförts, utgör en obligatorisk uppgift för LPID.

Den som driver enskild näringsverksamhet har däremot möjlighet att i, och genom, en tillhandahållen europeisk digital identitetsplånbok för fysiska personer lagra, respektive uppvisa, elektroniska attributsintyg som styrker behörighet att agera som företrädare för den enskilda näringsverksamheten.

³⁰ Det bör primärt vara en fråga för inblandade myndigheter att bestämma hur ett elektroniskt informationsutbyte organiseras mellan myndigheterna, jfr prop. 2019/20:106 s. 54 ff.

³¹ EU Digital Identity Wallet Consortium, se <https://eudiwalletconsortium.org/#>. Se även avsnitt 4.7.3.

Avgiftsuttag för tillhandahållande av uppgifter för personidentifiering att kopplas till den europeiska digitala identitetsplånboken för juridiska personer

Som redovisats inledningsvis (avsnitt 4.7.1) ska utfärdandet, användningen och återkallandet av europeiska digitala identitetsplånböcker vara utan kostnad för fysiska personer (se artikel 5a.13). Motsvarande begränsning finns enligt den reviderade eIDAS-förordningen inte för juridiska personer som vill ansöka om en europeisk digital identitetsplånbok eller tillhandahållande av uppgifter för personidentifiering som kan kopplas till densamma.

Anskaffandet av uppgifter om personidentifiering som kan kopplas till en europeisk identitetsplånbok för juridiska personer syftar till att tillgodose den enskilda organisationens behov. Även om full kostnadstäckning inte kommer att uppnås är det naturligt att tillhandahållandet av personidentifieringsuppgifter till den europeiska digitala identitetsplånboken för juridiska personer finansieras av användarna genom avgifter (se, för motsvarande bedömning avseende tillhandahållandet, avsnitt 6.3.1). Regeringen, eller efter regeringens bemyndigande, den myndighet som tillhandahåller uppgifter för personidentifiering för juridiska personer ska därför ges möjlighet att införa ett avgiftssystem. Närmare bestämmelser om avgiftssystemets utformning kan meddelas med stöd av förslaget bemyndigande som tas in i kompletteringslagen.

6.3.4 Elektroniska attributsintyg

Utredningens bedömning: Bestämmelserna om elektroniska attributsintyg i EU:s reviderade förordning om elektronisk identifiering är direkt tillämpliga och träffar bl.a. utfärdare av sådana intyg och förlitande parter. Det finns därmed inte anledning att genom ytterligare reglering på nationell nivå styra offentliga eller privata aktörer att utfärda, validera och godta elektroniska attributsintyg i enlighet med förordningens krav och förutsättningar.

Om behov skulle uppkomma finns möjligheter för regeringen att med andra styrmedel verka för att myndigheter och andra offentliga aktörer anpassar sina system och digitala tjänster för att uppfylla kraven beträffande elektroniska attributsintyg i den reviderade EU-förordningen och kommande genomförandeakter på området.

Skälen för utredningens bedömning

Som närmare redovisas i avsnitt 4.9.2 introduceras i den reviderade eIDAS-förordningen den nya betrodda tjänsten utfärdande av elektroniska attributsintyg samt validering av dessa intyg (se definition i artikel 3.18 g och 3.18 h). Elektroniska attributsintyg ska tillhandahållas till europeiska digitala identitetsplånböcker på ett sätt som möjliggör för en identitetsplånbok att efterfråga, hämta, lagra och hantera attributsintygen oavsett i vilket medlemsland som identitetsplånboken har tillhandahållits. Det är därför nödvändigt med harmoniserade referensstandarder, tekniska specifikationer och förfaranden för dessa tjänster och intyg, vilka kommer att fastställas av kommissionen i genomförandeakter.

Ett skäl för att den nya tjänsten införs är att det konstaterats att det föreligger hinder eller svårigheter för unionsmedborgare och invånare i unionen att på ett säkert sätt och med en hög nivå av dataskydd utbyta digital information över gränserna om sin identitet, såsom adress, ålder och yrkeskvalifikationer, körkort och andra tillstånd eller betalningsuppgifter.

Syftet är således att det ska bli möjligt att utfärda och hantera tillförlitliga elektroniska attribut att användas av unionsmedborgare och invånare i unionen i privata och offentliga transaktioner. Denna möjlighet kan antas bidra till att minska den administrativa bördan för användare. Vi menar att detta på sikt gäller även för förlitande parter som godtar den europeiska digitala identitetsplånboken i sina erbjudna tjänster.

Ett angivet exempel på användarfall är möjligheten att bevisa innehav av ett giltigt körkort utfärdat av en myndighet i en medlemsstat och som kan verifieras och godtas av bl.a. berörda myndigheter i andra medlemsstater. Det anges vidare att medborgare och invånare i EU bör även kunna förlita sig på sina uppgifter om social trygghet eller framtida digitala resehandlingar i ett gränsöverskridande sammanhang (skäl 54 i förordningens ingress, se även avsnitt 4.7.1 och figur 4.3).

Alla tillhandahållare av tjänster som utfärdar attesterade attribut i elektroniskt format, såsom examensbevis, licenser, personbevis eller befogenheter och uppdrag att företräda fysiska eller juridiska personer eller agera på deras vägnar anses enligt förordningen vara en tillhandahållare av betrodda elektroniska attributsintyg (skäl 55). Aktörer inom offentlig sektor kan vara utfärdare av elektroniska attributs-

intyg (såväl som parter som förlitar sig på sådana intyg). Det finns däremot inget uttryckligt krav på att offentliga aktörer själva *ska* utfärda elektroniska attributsintyg.

I likhet med övriga betrodda tjänster kan utfärdande och validering av elektroniska attributsintyg vara kvalificerade eller icke-kvalificerade, beroende på vilka krav som uppställs för tjänsten och dess tillhandahållare. Av definitionerna framgår vidare att attributsintygen i sig indelas i olika kategorier: elektroniskt attributsintyg (artikel 3.44), kvalificerat elektroniskt attributsintyg (artikel 3.45) och elektroniskt attributsintyg utfärdat av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa (artikel 3.46).

Attribut som baseras på autentiska källor (se definition av autentisk källa i artikel 3.47) ska kunna kontrolleras mot källan. Detta följer av artikel 45e i den reviderade eIDAS-förordningen. Av förordningens bilaga VI framgår en minimiuppsättning av sådana attribut. Det finns ingen yttre gräns för vilka attribut som kan komma att bli aktuella att använda och den europeiska digitala identitetsplånboken med dess attributsintyg skulle därmed på sikt kunna användas i bredare sammanhang än vad som följer av minimiuppställningen.³²

Enligt artikel 45e är det endast kvalificerade tillhandahållare av betrodda tjänster för elektroniska attributsintyg som, på begäran av en användare av europeisk digital identitetsplånbok, ska få kontrollera på elektronisk väg äktheten hos åtminstone attributen i minimiuppsättningen av attributen i nämnda bilaga. Sådana tillhandahållare står under tillsyn.

Kontroll av äktheten hos attributet får göras gentemot den relevanta autentiska källan på nationell nivå eller via särskilt utsedda mellanhänder som är erkända på nationell nivå i enlighet med unionsrätten eller nationell rätt.

Det är medlemsstaterna som ska säkerställa att åtgärder vidtas som gör den föreskrivna kontrollen möjlig. Sådana eventuella åtgärder ska vidtas inom 24 månader från ikraftträdandet av de genomförandeakter som avses i artiklarna 5a.23 och 5c.6. Sådana rättsakter ska antas senast den 21 november 2024.

För att Sverige ska efterleva förordningskraven behöver offentliga aktörer se över vilka autentiska källor som finns och som kan användas för utfärdande och kontroll av elektroniska attributsintyg. Dessa aktörer måste, i förekommande fall, också genomföra nödvän-

³² Se även Myndigheten för digital förvaltning, *Digital plånbok*, 2022-01-11, s. 13.

diga tekniska anpassningar för att efterleva kraven, som alltså följer direkt av förordningen och bestämmelser i kommande genomförandeakter.³³ Med hänsyn till den snäva tidsramen kan detta innebära en utmaning. Om behov uppstår kan det finnas anledning att överväga om det tidigare lämnade förslaget om en förvaltningsgemensam valideringstjänst för elektroniska underskrifter och stämplat bör utvidgas till att omfatta även validering av attributsintyg, i syfte att underlätta arbetet för offentliga aktörer.³⁴ Detta behöver dock utredas närmare i vederbörlig ordning, vilket inte ryms inom vårt uppdrag eller dess tidsram.

Offentliga aktörer ska i egenskap av förlitande parter därutöver, på användares begäran, godta europeiska digitala identitetsplånböcker med dess attributsintyg (också när det inte är fråga om gränsöverskridande användning). Med anledning av identitetsplånbokens modell för decentraliserade identitetslösningar kan även detta kräva förändringar av aktörernas tekniska system och erbjudna tjänster.

Skyldigheterna såvitt avser elektroniska attributsintyg framgår direkt av den reviderade eIDAS-förordningen. En förutsättning för att de aktörer som omfattas av skyldigheterna ska kunna tillämpa berörda bestämmelser är, som anförts, att de har anpassat sina tjänster och tekniska system efter uppställda krav. För närvarande finns inte anledning att genom ytterligare nationell författningsreglering styra offentliga eller privata aktörer att utfärda elektroniska attributsintyg, möjliggöra validering av attribut baserade på autentiska källor och godta elektroniska attributsintyg i enlighet med förordningens krav och förutsättningar. Vi bedömer att eventuellt behov av nationell reglering i syfte att exempelvis fastställa ytterligare ansvar och skyldigheter för berörda aktörer får övervägas först när kommissionen har antagit avsedda genomförandeakter på detta område.

Om det bedöms vara nödvändigt eller lämpligt kan regeringen även genom t.ex. regeringsuppdrag verka för att myndigheter – särskilt sådana som med författningsstöd ansvarar för berörda autentiska källor – anpassar sina system och digitala tjänster för att uppfylla den reviderade eIDAS-förordningens krav.

³³ För den fortsatta beredningen av lagstiftningsärendet har vi uppdragit åt Governo AB att göra en kartläggning av offentliga aktörer som berörs i artikel 45e i den reviderade eIDAS-förordningen, se bilaga 4 till detta slutbetänkande.

³⁴ *Vem kan man lita på?* (SOU 2021:9), s. 165 ff. Se även Myndigheten för digital förvaltning a.a. s. 25.

6.3.5 Kostnadsfria valideringsmekanismer

Utredningens förslag: Den myndighet regeringen bestämmer ska tillhandahålla

- en kostnadsfri valideringsmekanism som säkerställer att europeiska digitala identitetsplånböckers äkthet och giltighet kan kontrolleras.
- en kostnadsfri valideringsmekanism som gör det möjligt för användare av europeiska digitala identitetsplånböcker att kontrollera äkthet och giltighet för identiteten hos de förlitande parter som registrerats i enlighet med artikel 5b i EU:s reviderade förordning om elektronisk identifiering.

Utredningens bedömning: Föreslagna kostnadsfria valideringsmekanismer bör tillhandahållas av statliga myndigheter för att säkerställa att förordningens krav på angivna funktioner uppfylls över tid.

Den tillhandahållande myndigheten respektive tillsynsmyndigheten är lämpade att tillhandahålla valideringsmekanismerna.

Den tillhandahållande myndigheten bör ansvara för att – i enlighet med artikel 5a.18 d i EU:s reviderade förordning om elektronisk identifiering – informera kommissionen om den mekanism som gör det möjligt att validera de uppgifter för personidentifiering som avses i artikel 5a.5 f i nämnda förordning.

Skälen för utredningens förslag och bedömning

Medlemsstaterna ska tillhandahålla kostnadsfria valideringsmekanismer

Enligt förordningens artikel 5a.8 ska medlemsstaterna tillhandahålla kostnadsfria valideringsmekanismer för de europeiska digitala identitetsplånböckerna. Funktionen validering definieras i förordningen som en process genom vilken det kontrolleras och bekräftas att data i elektronisk form är giltiga i enlighet med förordningen (artikel 3.41).

Valideringsmekanismerna ska tillhandahållas av medlemsstaterna i syfte att a) säkerställa att europeiska digitala identitetsplånböckers äkthet och giltighet kan kontrolleras och b) göra det möjligt för an-

vändare av europeiska digitala identitetsplånböcker att kontrollera äkthet och giltighet för identiteten hos de förlitande parter som registrerats i enlighet med artikel 5b (artikel 5a.8).³⁵

Medlemsstaterna ska informera kommissionen om de båda valideringsmekanismerna – liksom en valideringsmekanism för uppgifter för personidentifiering (se mer om denna mekanism nedan) – utan onödigt dröjsmål (artikel 5a.18 d och 5a.18 e).

Enligt vår bedömning finns det inga bestämmelser i förordningen som medför att en viss aktör bör tilldelas ansvaret för att tillhandahålla de kostnadsfria valideringsmekanismerna. För att säkerställa att de angivna mekanismerna kontinuerligt finns tillgängliga för kostnadsfri användning anser vi emellertid att statliga myndigheter ska ansvara för att tillhandahålla dem. Det framstår då som ändamålsenligt att valideringsmekanismen som säkerställer att europeiska digitala identitetsplånböckers äkthet och giltighet kan kontrolleras tillhandahålls av den myndighet som ansvarar för att tillhandahålla den digitala identitetsplånboken. På samma sätt är det ändamålsenligt att tillsynsmyndigheten tillhandahåller valideringsmekanismen som gör det möjligt för användare av europeiska digitala identitetsplånböcker att kontrollera äkthet och giltighet för identiteten hos de förlitande parter som registrerats i enlighet med artikel 5b, eftersom myndigheten föreslås ansvara för registret över förlitande parter.

Kommissionen ska även informeras om den mekanism som gör det möjligt att validera personidentifieringsuppgifter

I det förslag till reviderad förordning som kommissionen presenterade den 3 juni 2021 angavs i artikel 6a.5 (i den reviderade eIDAS förordningen artikel 5a.8) att medlemsstaterna skulle tillhandahålla vissa valideringsmekanismer. Bland dessa angavs i punkten 5c en valideringsmekanism för att göra det möjligt för förlitande parter och tillhandahållare av betrodda tjänster att kontrollera äktheten och giltigheten för personidentifieringsuppgifter med attribut.³⁶ I den reviderade eIDAS-förordningen kvarstår inte längre något krav på att

³⁵ Se mer om registret över förlitande parter i avsnitt 6.6.2.

³⁶ Förslag till Europaparlamentets och rådets förordning om ändring av förordning [EU] nr 910/2014 vad gäller inrättandet av en ram för europeisk digital identitet, COM[2021] 281 final av den 3 juni 2021.

medlemsstaterna ska tillhandahålla en mekanism för att validera personidentifieringsuppgifter.

Som ovan angetts ska emellertid medlemsstaterna utan onödigt dröjsmål – utöver de båda kostnadsfria valideringsmekanismerna – informera kommissionen om den mekanism som gör det möjligt att validera de personidentifieringsuppgifter som avses i artikel 5a.5 f (se artikel 5a.18 d).

Vi har inte kunnat utläsa eller efter gjorda efterforskningar fått någon förklaring till vad som föranledde att medlemsstaterna inte längre ska tillhandahålla denna mekanism men trots detta anmäla densamma. Utifrån att det alltså finns ett krav om att medlemsstaten ska informera kommissionen om nämnda mekanism gör vi bedömningen att det framstår som mest ändamålsenligt att den av regeringen utsedda myndigheten som ska tillhandahålla den europeiska digitala identitetsplånboken fullgör ifrågavarande informationsskyldighet i förhållande till kommissionen.

Mot bakgrund av vår bedömning att Digg bör utses till tillhandahållare av den europeiska digitala identitetsplånboken (avsnitt 6.3.1), kan det konstateras att ansvaret att informera kommissionen ligger väl i linje med myndighetens nuvarande uppgifter (se 7 § förordningen med instruktion för Myndigheten för digital förvaltning).

6.3.6 Tillhandahållande av förteckningar för validering

Utredningens bedömning: Tillhandahållare av den europeiska digitala identitetsplånboken, tillhandahållaren av registret över förlitande parter och tillhandahållare av uppgifter för personidentifiering ansvarar – som en del av tillhandahållandet – för att möjliggöra validering av det som tillhandahålls.

Skälen för utredningens bedömning

I ARF:en beskrivs det som vi valt att kalla tillhandahållande av förteckningar för validering (se avsnitt 4.7.4). Exempelvis är i avsnitt 6.3.5 nämnda kostnadsfria valideringsmekanismer beroende av att det finns förteckningar över tillhandahållare av identitetsplånböcker och en förteckning för registret över förlitande parter mot vilka validering

kan ske. Den validering som görs mot förteckningarna är för att t.ex. kontrollera att en europeisk digital identitetsplånbok är äkta och godkänd eller för att kunna se att en förlitande part är registrerad för att komma åt identitetsuppgifter eller attribut från en identitetsplånbok. Exakt vad som ska finnas i förteckningarna och hur valideringen ska gå till är i skrivande stund oklart. Formerna för, och eventuella begränsningar för medlemsstaterna i utformningen av förteckningarna, kommer att omfattas av de genomförandeakter som EU-kommissionen ska ta fram enligt artikel 5a.23 senast den 21 november 2024.

Trots att det finns betydande osäkerheter kring hur förteckningarna ska utformas och valideringen ska gå till bedömer vi att vi behöver ta ställning till hur ansvaret för att tillhandahålla de aktuella förteckningarna ska placeras.

Enligt vår uppfattning får det anses naturligt att förteckningen över tillhandahållare av europeiska digitala identitetsplånböcker sköts av den myndighet som tillhandahåller och godkänner identitetsplånböcker. Av samma anledning bör förteckningen över registret av förlitande parter hållas av den som ansvarar för registret.

Kvalificerade attributsintyg är en kvalificerad betrodd tjänst och omfattas således av den tillitsförteckning för kvalificerade betrodda tjänster som avses i artikel 22 i eIDAS-förordningen med tillhörande genomförandeakt.³⁷ Detta framgår även av ARF:en.³⁸ Tjänsten tillhandahållande av attributsintyg från autentisk källa påminner mycket om tjänsten kvalificerade elektroniska attributsintyg. Kraven i artikel 45f.2 i den reviderade eIDAS-förordningen innebär att de offentliga organ som utfärdar elektroniska attributsintyg ska ha en tillförlitlighetsnivå som är likvärdig med den hos kvalificerade tillhandahållare av betrodda tjänster. Det finns även krav på att organen ska certifieras i enlighet med punkten 3 i samma artikel. Kraven på certifieringen kommer att omfattas av en genomförandeakt som EU-kommissionen ska ta fram till senast den 21 november 2024 som ska omfatta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden enligt artikel 45f.7. Tillitsförteckningar enligt genomförandebeslutet får även innehålla icke-kvalificerade till-

³⁷ Kommissionens genomförandebeslut (EU) 2015/1505 av den 8 september 2015 om fastställande av tekniska minimispecifikationer och format rörande förteckningar över betrodda tjänsteleverantörer i enlighet med artikel 22.5 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden.

³⁸ The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework – Architecture and Reference Framework, version 1.4.0, avsnitt 3.4.

handahållare av betrodda tjänster och icke-kvalificerade betrodda tjänster.³⁹ För dessa tjänster kan validering alltså ske med den tillitsförteckning som tillhandahålls av PTS.

Vad gäller tillhandahållare av PID anges i ARF:en att även dessa ska omfattas av tillitsförteckningen.⁴⁰ Tillhandahållare av PID eller LPID är emellertid inte tillhandahållare av kvalificerade betrodda tjänster och det finns inga nu publicerade bestämmelser som ger stöd till att de kan tas med i tillitsförteckningen. Som framgår av avsnitt 6.3.5 är den i skrivande stund tillgängliga informationen om valideringsmekanismer kring PID och LPID oklar och delvis motsägelsefull. Enligt vår uppfattning får det emellertid anses vara en rimlig följd av själva tillhandahållandet av PID/LPID att det även innefattar att möjliggöra validering. Antingen genom att ansvarig aktör möjliggör sådan validering genom en egen förteckning eller genom tillitsförteckningen eller liknande lösning som möjliggörs av det kommande regelverket.

I ARF:en nämns, utöver de ovan listade förteckningarna, en förteckning över certifikatutfärdare som utfärdar certifikat till vissa tillhandahållare (se avsnitt 4.7.4).⁴¹ Eftersom dessa certifikat utfärdas till respektive tillhandahållare är det tillhandahållaren som, oavsett certifikatets ursprung, i likhet med vad som anges ovan får anses ansvarig för att validering möjliggörs av det som tillhandahålls.

³⁹ Kommissionens genomförandebeslut (EU) 2015/1505 av den 8 september 2015 om fastställande av tekniska minimispecifikationer och format rörande förteckningar över betrodda tjänsteleverantörer i enlighet med artikel 22.5 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden, art. 2 sid. 2.

⁴⁰ The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework – Architecture and Reference Framework, version 1.4.0, avsnitt 3.4.

⁴¹ Ibid.

6.3.7 Certifiering av den digitala europeiska identitetsplånboken och system för elektronisk identifiering

Utredningens förslag: Regeringen eller den myndighet som regeringen bestämmer ska utse ansvarigt organ för certifiering av europeiska digitala identitetsplånböcker och system för elektronisk identifiering.

Utredningens bedömning: Certifieringsorgan som är ackrediterade enligt cybersäkerhetsakten är bäst lämpade att genomföra certifiering av den europeiska digitala identitetsplånboken.

Försvarets materielverk är bäst lämpad att ansvara för att utse organ för certifiering av europeiska digitala identitetsplånböcker och system för elektronisk identifiering i Sverige.

Myndigheten för digital förvaltning är bäst lämpad att ta fram en eventuell nationell certifieringsordning med krav som inte omfattas av kraven i cybersäkerhetsakten.

Skälen för utredningens förslag och bedömning

Bakgrund

Att den europeiska digitala identitetsplånboken överensstämmer med förordningen ska certifieras av ett, av varje medlemsstat, utsett organ för bedömning av överensstämmelse. Certifieringen ska vara giltig i högst fem år och villkoras av att en sårbarhetsbedömning genomförs med intervall om två år (artikel 5c.1–3 och 4).

Certifiering av att identitetsplånböckerna överensstämmer med cybersäkerhetskrav ska genomföras i enlighet med de cybersäkerhetssystem som antagits i enlighet med de europeiska certifieringsordningar för cybersäkerhet som antagits med stöd av Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten).

För de krav som inte rör cybersäkerhet eller som inte omfattas av kraven i nyss nämnda förordning ska medlemsstaterna etablera nationella certifieringsordningar som uppfyller kraven i kommissionens genomförandeakt till den reviderade eIDAS-förordningen. Medlems-

staterna ska överföra sitt nationella förslag på certifieringsordning till den europeiska samarbetsgruppen för digital identitet (EDICG) som kommissionen etablerat. EDICG får utfärda synpunkter och rekommendationer (artikel 5c.3).

Medlemsstaterna ska informera kommissionen och EDICG om vilka identitetsplånböcker som har utfärdats och certifierats av utpekad organ för bedömning av överensstämmelse samt om – och i sådant fall varför – en certifiering avbryts (artikel 5d.1). Den information som lämnas ska åtminstone innehålla uppgifter om certifikat och bedömningsrapport från den certifierade identitetsplånboken, en beskrivning av den digitala identitetskontrollen i samband med utfärdandet, tillämplig tillsyns- och ansvarsordning för tillhandahållaren av identitetsplånboken, vilka myndigheter som ansvarar för den digitala identitetskontrollen och tillvägagångssätt vid avstängning eller återkallelse av system för elektronisk identifiering, autentisering eller äventyrade delar av det anmälda systemet som föranlett ett tillfälligt upphävande eller återkallelse (artikel 5d.2).

Utifrån den information som lämnas ska kommissionen upprätta, offentliggöra, underhålla och uppdatera en maskinläsbar lista över certifierade europeiska digitala identitetsplånböcker (artikel 5d.3).

Certifieringen av identitetsplånboken bygger som ovan framgått främst på certifiering enligt cybersäkerhetsakten och merparten av kraven är cybersäkerhetskrav. I Sverige är Försvarets materielverk (FMV) nationell myndighet för cybersäkerhetscertifiering enligt cybersäkerhetsakten.⁴² Ramverket för cybersäkerhetscertifiering är under etablering och de organ för bedömning av överensstämmelse, såsom certifieringsorgan, kommer att kunna etableras och ackrediteras enligt den första certifieringsordningen för IKT-produkter baserat på Kommissionens genomförandeförordning (EU) 2024/482 av den 31 januari 2024 om fastställande av tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) 2019/881 vad gäller antagande av den europeiska Common Criteria-baserade ordningen för cybersäkerhetscertifiering (EUCC) som trädde i kraft i februari 2024. Cybersäkerhetsakten innebär att en stor del av den certifiering som i dag sker av statliga certifieringsorgan inom EU fr.o.m. den 27 februari 2025 i stället kommer utföras av privata certifieringsorgan när de första EUCC-certifikaten kan börja utfärdas. FMV, genom Sveriges Certifieringsorgan för IT-säkerhet (CSEC) som är en del av

⁴² 3 § förordningen (2021:555) med kompletterande bestämmelser till EU:s cybersäkerhetsakt.

FMV, får enligt EUCC enbart ta emot nya ansökningar inom nuvarande överenskommelser (SOG-IS⁴³ och CCRA⁴⁴) fram t.o.m. den 26 februari 2025. CSEC måste därför slutföra alla certifieringar, inom de nuvarande överenskommelserna, innan den 27 februari 2026. Då ska nuvarande verksamhet enligt artikel 49 i EUCC upphöra att ha verkan. Detta innebär att CCRA och SOG-IS certifieringar därefter inte kommer utföras i Sverige (eller inom EU).

Samtliga certifikat som utfärdas inom EUCC, och även kommande certifieringsordningar under cybersäkerhetsakten, kommer ha samma verkan inom hela EU oavsett vilket organ för bedömning av överensstämmelse som utfärdar det i ett EU-land, så länge som organet uppfyller tillämpliga krav. Sverige måste därmed erkänna certifikat utfärdade av privata eller statliga organ i andra medlemsstater för bedömning av överensstämmelse.

Inom EUCC finns det två assurancesnivåer. Det är nivå betydande ("substantial") där certifieringar helt och hållet kommer utfärdas av privata certifieringsorgan som uppfyller kraven för ackreditering och är ackrediterade av det nationella ackrediteringsorganet. I Sverige är Swedac det nationella ackrediteringsorganet. Den andra assurancesnivån är nivå hög ("high") där certifiering antingen kan utföras av ett statligt organ för bedömning av överensstämmelse, efter ett förhandsgodkännande eller allmän delegering av den nationella myndigheten för cybersäkerhetscertifiering, eller av privata organ för bedömning av överensstämmelse. Både de privata och statliga organen ska utöver ackrediteringen också bli bemyndigade av den nationella myndigheten för cybersäkerhetscertifiering.

Merparten av de certifieringar som CSEC utför i dag är på nivå väsentlig. För att certifiera hårdvara på nivå hög enligt EUCC tillkommer ytterligare krav. Det är enbart ett fåtal länder i Europa som gör detta i dag, och enligt uppgift kan sådan certifiering i skrivande stund endast utföras i Tyskland, Nederländerna, Frankrike och Spanien.

De certifieringar som CSEC gör i dagsläget sker inom de andra överenskommelser som nu kommer ersättas av EUCC. Därför sker nu en överflyttning från statliga till privata organ. De tekniska domänerna som t.ex. smarta kort och hårdvara på assurancesnivå hög är inget som det i Sverige i dagsläget finns kompetens för att certifiera, eller

⁴³ SOG-IS står för Senior Officials Group of Information Systems Security, som bl.a. hanterar överenskommelse om ömsesidigt erkännande av it-säkerhetscertifieringar inom EU.

⁴⁴ CCRA står för "Common Criteria Recognition Agreement".

med tanke på den begränsade marknaden, troligtvis kommer att kunna bygga upp. Detta då det kräver både särskild utrustning och kompetens, något som är både svårt att få fram och mycket resurskrävande. Det är därför ett rimligt antagande att det även fortsättningsvis endast kommer att vara ett begränsat antal EU-länder som kommer utföra denna typ av certifieringar.

Vilken eller vilka assurancesnivåer som certifieringen av den europeiska digitala identitetsplånboken kommer att kräva är för närvarande okänd eftersom det kommer att fastställas i de genomförandakter som omfattar kraven på certifiering i enlighet med artikel 5c.6.

Sverige måste utse ett organ för certifiering

Förordningen uppställer ett krav på att Sverige ska utse ett organ för certifiering av europeiska digitala identitetsplånböcker (artikel 5c.1). Trots det ovan beskrivna nuläget där det finns flera osäkra faktorer måste vi från utredningens sida föreslå hur Sverige ska uppfylla detta krav.

Skyldigheten i den reviderade eIDAS-förordningen avser att utse ett organ för bedömning av överensstämmelse. Certifieringsorgan som är ackrediterade enligt cybersäkerhetsakten är bäst lämpade att genomföra certifiering av den digitala identitetsplånboken. Kravet i förordningen om att utse ett organ får anses innebära att både statliga och privata organ kan utses. Någon begränsning vad gäller att organet måste vara svenskt kan inte heller anses föreligga. Det går emellertid inte, med den osäkerhet som nu råder, att närmare peka ut vilket eller vilka organ som skulle utfärda de nödvändiga certifieringarna. Ett bemyndigande om att regeringen, eller den myndighet som regeringen bestämmer, ska få utse ett organ för certifiering av europeiska digitala identitetsplånböcker ska därför tas in i kompletteringslagen.

Vi bedömer att FMV som nationell myndighet för cybersäkerhetscertifiering är bäst lämpad att utse ett sådant organ. Formerna för hur ett sådant organ utses kan variera beroende på de förutsättningar som råder, t.ex. om det krävs att FMV initierar ett upphandlingsförfarande. I ett scenario där det saknas möjlighet att utse ett ackrediterat certifieringsorgan i antingen Sverige eller något annat EU-land kan FMV även i teorin utse att myndigheten på egen hand ska utföra certifieringen. Ett sådant utfall framstår emellertid som mindre troligt.

Ansvar för certifiering av system för elektronisk identifiering samt en eventuell nationell certifieringsordning

Certifiering av system för elektronisk identifiering i enlighet med (artikel 12a) omfattar främst cybersäkerhetskrav liknande de som finns för den europeiska digitala identitetsplånboken och hänvisar, på samma sätt som i fråga om identitetsplånboken, till cybersäkerhetsakten. Det anges även att certifieringen ska ske inom ramen för en relevant ordning för cybersäkerhetscertifiering enligt cybersäkerhetsakten (artikel 12a.2). Detta medför att det kan komma att vara samma ordning för system för elektronisk identifiering som för identitetsplånboken om ordningen som tas fram passar för båda. Om det blir samma ordning innebär detta att det vore möjligt att hålla ansvaret för certifieringen av identitetsplånboken och system för elektronisk identifiering samlad. Vi bedömer därmed att FMV även bör tilldelas ansvaret för certifiering av system för elektronisk identifiering.

Det finns visst utrymme för nationella certifieringsordningar enligt artikel 5c.3; dessa ska emellertid bygga på genomförandeakter till den reviderade eIDAS-förordningen. I dessa genomförandeakter, som ska antas senast den 21 november 2024, kommer referensstandarder och vid behov specifikationer och förfaranden pekats ut. Det är därför ytterst tveksamt om det finns behov av eller om det ens hinner utarbetas svenska certifieringsordningar baserade på andra standarder eller specifikationer än de som kommer att pekats ut i genomförandeakterna. För det fall att det ändå kan bli aktuellt med en nationell certifieringsordning bedömer vi att Digg bör ansvara för att ta fram en nationell certifieringsordning för europeiska digitala identitetsplånböcker som omfattar andra områden än cybersäkerhet. Eftersom det inte är troligt att en sådan nationell ordning kommer behöva tas fram lämnar vi emellertid inget förslag i denna del.

Certifieringsordningen kan dock även omfatta de krav på cybersäkerhet som inte täcks av någon cybersäkerhetscertifieringsordning enligt cybersäkerhetsakten. Certifieringsordningen kan användas för nationell certifiering av identitetsplånböcker. De krav som ska vara uppfyllda hänger nära samman med tillhandahållandet av europeiska digitala identitetsplånböcker och möjligt erkännande av plånböcker från privata aktörer (se avsnitt 6.3.1). Det finns också beröringspunkter med Diggs arbete med krav på aktörer och e-legitimationssystem som har anmält sig till det auktorisationssystem för elektronisk iden-

tifiering och för digital post som tillhandahålls av Digg. Diggs tillitsramverk för Svensk e-legitimation kommer vidare sannolikt att kunna ligga till grund för en sådan certifieringsordning för digitala identitetsplånböcker och möjlig certifieringsordning för system för elektronisk identifiering enligt artikel 12a.

6.3.8 Tillhandahållandet förutsätter att åtgärder för ökad illgänglighet vidtas

Utredningens bedömning: För att tillgodose kraven i EU:s reviderade förordningen om elektronisk identifiering avseende lika tillgång till digital identifiering för alla medborgare och invånare behöver tillgänglighetsanpassningar genomföras och åtgärder kopplade till ställföreträdarens uppdrag att företräda annan vidtas.

Skälen för utredningens bedömning

Åtgärder som möjliggör ökad tillgänglighet behöver vidtas

Den reviderade eIDAS-förordningen uppställer en rad krav på den europeiska digitala identitetsplånboken ur ett tillgänglighetsperspektiv. Tillhandahållaren ska bland annat säkerställa att användarna enkelt kan begära tekniskt stöd och rapportera tekniska problem eller andra incidenter som har en negativ inverkan på användningen av den europeiska digitala identitetsplånboken (artikel 5a.10). Vidare ska identitetsplånboken göras tillgänglig för användning av personer med funktionsnedsättning, på samma villkor som andra användare (artikel 5a.21). Vikten av lika tillgång till digital identifiering för alla medborgare och invånare i en medlemsstat kommer till uttryck även i artikel 15 liksom i förordningens ingress (se t.ex. skäl 15, 35 och 43). För att tillgodose dessa krav behöver de aspekter som vi i vårt delbetänkande framhöll för att skapa ökad tillgänglighet till en statlig e-legitimation beaktas. Det kan exempelvis vara fråga om hjälpmedel, teknisk support och informationskampanjer.⁴⁵

Förordningen föreskriver också att en europeisk digital identitetsplånbok ska säkerställa att personidentifieringsuppgifter som avser

⁴⁵ *En säker och tillgänglig statlig e-legitimation* (SOU 2023:61), s. 99 ff., 132 f. och 312 ff.

en fysisk person som företräder en annan fysisk person är kopplade till den europeiska digitala identitetsplånboken (jfr artikel 5a.5 f). En sådan koppling skulle vara värdefull vid gode mäns och förvaltares uppdrag som ställföreträdare. En tillförlitlig koppling förutsätter emellertid att det finns säkerställda uppgifter som kan utgöra underlag för förekomsten av ett ställföreträdarskap och dess omfattning. Detta eftersom sådana omständigheter kan förändras över tid. Ett sätt att åstadkomma en sådan koppling skulle kunna vara ett nationellt register över ställföreträdare. För närvarande finns inget sådant register men ett förslag om att inrätta ett, tillsammans med andra åtgärder, har lämnats av Ställföreträdarutredningen, vars förslag bereds i Regeringskansliet.⁴⁶ I vårt delbetänkande anslöt vi oss till den utredningens bedömning att exempelvis ett nationellt register över förordnade förmyndare, gode män och förvaltare samt de som har en sådan ställföreträdare, var nödvändigt för att huvudmän skulle kunna få tillgång till e-legitimation och digitala tjänster i större utsträckning än vad som nu är möjligt.⁴⁷ Detsamma gäller enligt vår bedömning för att tillgängliggöra den europeiska digitala identitetsplånboken på ett säkert sätt. Vid den fortsatta beredningen av dessa frågor finns anledning att överväga om de bör samordnas med arbetet kopplat till skyddet för vuxna i gränsöverskridande situationer.⁴⁸

⁴⁶ *Gode män och förvaltare – en översyn* (SOU 2021:36), s. 427 ff.

⁴⁷ *En säker och tillgänglig statlig e-legitimation* (SOU 2023:61), s. 133. Behovet framhålls också i Funktionsrätt Sveriges remissvar över delbetänkandet. Organisationen påpekar att det är av yttersta vikt att ställföreträdare som hjälper sin huvudman kan använda e-legitimationen för att undvika att personer med funktionsnedsättning fortsatt blir utestängda från det digitala samhället.

⁴⁸ Förslag till rådets förordning om gemensamma regler i EU om behörig domstol, tillämplig lag och ömsesidigt erkännande av åtgärder till skydd för utsatta vuxna vid gränsöverskridande situationer och om inrättandet av ett europeiskt fullmaktsintyg och sammankoppling av myndigheters register, COM (2023) 280 final av den 31 maj 2023.

6.3.9 Behandling av personuppgifter

Utredningens förslag: I lagen med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering ska införas centrala bestämmelser om den behandling av personuppgifter som är nödvändig i verksamheten för det statliga tillhandahållandet av den europeiska digitala identitetsplånboken och den databas som ska föras över sådana identitetsplånböcker. Vidare ska lagen innehålla ett undantag från rätten att invända mot personuppgiftsbehandling som framgår av artikel 21 i EU:s dataskyddsförordning.

I integritetshöjande syfte tas i lagen även in en bestämmelse om sökbegränsningar som rör uppgifter om lagöverträdelser.

En upplysning införs om att de nya bestämmelserna om behandling av personuppgifter kompletterar EU:s dataskyddsförordning och lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

Därutöver ska lagen innehålla bemyndigande för regeringen eller den myndighet som regeringen bestämmer att meddela närmare föreskrifter om dels innehållet i databasen över tillhandahållna europeiska digitala identitetsplånböcker, dels om en högsta lagringstid (tio år) för uppgifter i databasen.

Utredningens bedömning: Den behandling av personuppgifter som aktualiseras vid tillhandahållande av sådana uppgifter för personidentifiering som ska kopplas till en europeisk digital identitetsplånbok, liksom den som sker i samband med att tillsynsmyndigheten över europeiska digitala identitetsplånböcker för ett register över förlitande parter, kräver inte någon nationell författningsåtgärd.

Skälen för utredningens förslag och bedömning

Utgångspunkter för behandling av personuppgifter

Våra förslag innebär att personuppgifter behandlas. Förslagen måste därför bedömas med beaktande av att det i 2 kap. 6 § andra stycket regeringsformen fastslås att var och en gentemot det allmänna ska skyddas mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av

den enskildes personliga förhållanden. Inskränkningar i denna rättighet får bara ske genom lag och bara under vissa förutsättningar (2 kap. 20 och 21 §§ regeringsformen).

Den reglering som vi föreslår måste vidare vara förenlig med Europeiska unionens stadga om de grundläggande rättigheterna (EU:s rättighetsstadga). I artikel 7 i stadgan tryggas respekten för privatlivet och i artikel 8 fastslås rätten till skydd av personuppgifter. Ett sådant skydd föreskrivs även i Europeiska konventionen om skydd för de mänskliga rättigheterna (Europakonventionen). Av artikel 8 i Europakonventionen följer rätten för envar att åtnjuta respekt för sitt privat- och familjeliv. I Europadomstolens rättspraxis har artikeln ansetts omfatta skyddet av personuppgifter.

Regler om skydd för personuppgifter finns vidare i EU:s dataskyddsförordning. Förordningen är direkt tillämplig i varje medlemsstat, men både förutsätter och tillåter att det i vissa fall finns nationella bestämmelser som kompletterar eller utgör undantag från förordningens regler. I Sverige finns sådana bestämmelser bl.a. i lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

All behandling av personuppgifter måste vara förenlig med de allmänna principer som anges i artikel 5.1 i EU:s dataskyddsförordning. Dessa innebär bl.a. att personuppgifter ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade, samt att uppgifter bara får samlas in för vissa särskilda och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål.

Utöver de allmänna principerna utgår EU:s dataskyddsförordning från att varje behandling av personuppgifter ska vila på åtminstone en av de rättsliga grunder som uttömmande anges i artikel 6.1 i förordningen.

De bestämmelser om behandlingen av personuppgifter som vi föreslår i detta betänkande har sin grund i det nationella handlingsutrymmet enligt artikel 6 i EU:s dataskyddsförordning. Detta utrymme är begränsat. Det krävs att medlemsstaternas lagstiftning kan anses dels uppfylla ett mål av allmänt intresse, dels stå i proportion till det legitima mål som eftersträvas. Om personuppgifter behandlas för annat ändamål än det för vilket personuppgifterna ursprungligen samlades in, ska bestämmelserna bedömas mot principen om ändamålsbegränsning på det sätt som anges i artikel 6.4 i EU:s dataskyddsförordning.

förordning. Bestämmelserna ska vara en nödvändig och proportionell åtgärd för att skydda de mål som avses i artikel 23.1 i förordningen. Bestämmelserna ska också stå i proportion till det legitima mål som eftersträvas. I sådana nationella bestämmelser ska till centrala delar rätten till skydd för personuppgifter iakttas, och det ska föreskrivas om lämpliga och särskilda åtgärder för att skydda den registrerades grundläggande rättigheter och intressen.

Enligt artikel 6.1 c i EU:s dataskyddsförordning är behandling av personuppgifter tillåten, dvs. anses ha laglig grund, om behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige. Behandlingen av personuppgifter är enligt artikel 6.1 e även laglig om den är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.

Personuppgiftsbehandling som utförs i samband med den statligt tillhandahållna europeiska digitala identitetsplånboken

Som framgått råder i skrivande stund oklarhet om vilken eller vilka tekniska lösningar som kommer att bli aktuella för att skapa tillit i ekosystemet för den europeiska digitala identitetsplånboken. Först när harmoniserad reglering om tillitsmodell för den europeiska digitala identitetsplånboken finns på plats kommer det att stå klart vilket behov som finns av att uppgifter om tillhandahållna identitetsplånböcker och deras användare tas in i ett register. Vi bedömer emellertid för närvarande att återkallelse av en identitetsplånboksinstans, tillika tillgängliggörande av information om dess status för att möjliggöra validering, förutsätter att tillhandahållaren på något sätt har uppdaterad information om tillhandahållna identitetsplånböcker. I våra överväganden har vi därför utgått från att tillhandahållare av den europeiska digitala identitetsplånboken behöver föra någon form av egen förteckning eller register, och lämnar därför författningsförslag till stöd för detta.

Vi har föreslagit att regeringen utser en myndighet med uppdrag att tillhandahålla en europeisk digital identitetsplånbok med stöd av artikel 5a.2 a och 5a.2 b. Den tillhandahållande myndigheten har att på eget ansvar uppfylla kraven på föreskrivna plånboksfunktioner. Vidare är myndigheten ansvarig för att de uppgifter om användarna som är nödvändiga (och tillåtna) för att tillhandahålla plånbokstjänst-

erna finns samlade. Därmed föreligger personuppgiftsansvar för verksamheten och en skyldighet att efterleva reglerna om personuppgiftsbehandling i EU:s dataskyddsförordning, såväl som bestämmelserna om integritetsskydd som föreskrivs i den reviderade eIDAS-förordningen.

Vi bedömer att nödvändig behandling av personuppgifter för den tillhandahållande myndigheten av identitetsplånböcker, inbegripet upprättande och förvaltning av databaser, har stöd i de villkor som fastslås i artikel 6.1 i dataskyddsförordningen, primärt i artikel 6.1 c eller 6.1 e.

Uppgiften att tillhandahålla en europeisk digital identitetsplånbok är av allmänt intresse, och den personuppgiftsbehandling som uppgiften förutsätter är även nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige. Det är av avgörande betydelse att det går att säkerställa att en fysisk (eller juridisk) person kan kopplas till en viss identitetsplånbok vid tillhandahållandet. Vidare får det, som redan framhållits, bedömas vara nödvändigt att den tillhandahållande myndigheten för en databas för att bl.a. hantera en återkallelse av giltigheten av en tillhandahållen digital identitetsplånbok och möjliggöra validering av densamma (se mer om valideringen i avsnitt 6.3.5). Eftersom vårt förslag innebär att verksamheten att tillhandahålla en identitetsplånbok författningsregleras, kommer – i enlighet med kraven i EU:s dataskyddsförordning – den rättsliga grunden att framgå av såväl unionsrätt som nationell rätt.

De personuppgifter som myndigheten behöver registrera för att tillhandahålla en identitetsplånbok för fysiska personer är användarens fullständiga namn, identitetsbeteckning (personnummer eller samordningsnummer för personer med styrkt identitet), födelsetid och uppgifter om den e-legitimation med vilken användaren styrkt sin identitet för anslutning till och ibruktage ("onboarding") av identitetsplånboken.

I den föreslagna databasen kommer behandling att ske av personuppgifter som redan finns i befintliga myndighetsregister, primärt folkbokföringsdatabasen och i databasen över statliga e-legitimationer, om det förslaget genomförs.⁴⁹ Registerförande myndighet har (respektive har föreslagits ha) laglig grund för att tillgängliggöra relevanta uppgifter om behandling. Som framgått tillhandahålls redan flera myn-

⁴⁹ *En säker och tillgänglig statlig e-legitimation* (SOU 2023:61), s. 209 ff.

digheter uppgifter från Skatteverkets folkbokföringsdatabas (se avsnitt 6.3.3).

Utöver nämnda personuppgifter kommer databasen också att behöva innehålla uppgift som på ett unikt sätt identifierar tillhandahållna identitetsplånböcker (identitetsplånboксinstanser). Slutligen är det nödvändigt att i databasen införa uppgifter om giltighetstid och status, såsom uppgift om giltigheten av identitetsplånboken är återkallad och skälen för det.

De personuppgifter som är nödvändiga att behandla för tillhandahållandet av den digitala identitetsplånboken omfattas inte av dataskyddsförordningens särskilda kategorier av personuppgifter (s.k. känsliga personuppgifter). Även om person- och samordningsnummer inte i och för sig utgör känsliga personuppgifter anses dessa ändå vara en typ av uppgifter som förtjänar ett särskilt skydd. Av 3 kap. 10 § dataskyddslagen framgår att person- och samordningsnummer får behandlas utan samtycke endast när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl. I verksamheten med att tillhandahålla den europeiska digitala identitetsplånboken är vikten av en säker identifiering uppenbar. Det finns således stöd för att behandla person- och samordningsnummer utan sådant samtycke enligt nämnda lagrum och någon särskild bestämmelse behöver inte införas.

När det gäller europeiska digitala identitetsplånböcker till juridiska personer (även benämnda organisationsplånböcker) är det i huvudsak inte fråga om personuppgifter som kommer att behöva behandlas. Uppgifter som behöver hanteras, och registreras i databasen, är uppgift om den juridiska personens organisationsnummer, samt de för fysiska personer tidigare nämnda övriga uppgifter, dvs. sådana som kan identifiera den tillhandahållna plånboксinstansen och dess status. Som vi återkommer till i det följande kan det dock bli aktuellt att också behandla personuppgifter såsom namn på behörig firma-tecknare för den juridiska personen i fråga.

Vi föreslår således att det i kompletteringslagen införs bestämmelser som tillåter den behandling av personuppgifter som är nödvändig i verksamheten för det statliga tillhandahållandet av den europeiska digitala identitetsplånboken och i den databas som ska föras över sådana identitetsplånböcker. Detta innefattar exempelvis att säkerställa att inte flera identitetsplånböcker tillhandahålls till samma person. Formuleringen innehåller en sådan generell skrivning som har ansetts

tillräcklig exempelvis i lagen om identitetskort för folkbokförda (se 12 § nämnda lag).

Personuppgifter som behandlas i verksamheten med tillhandahållandet av den europeiska digitala identitetsplån boken kan även behöva behandlas för att kunna lämnas ut till andra myndigheter eller till enskilda. Vid en avvägning mellan intresset av utlämnande och intresset av att skydda de registrerades integritet bedömer vi, med beaktande särskilt av de berörda uppgifternas art, att intresset för att möjliggöra ett utlämnande väger tyngre. En bestämmelse som tillåter behandling av personuppgifter för det nämnda sekundära ändamålet införs därför i kompletteringslagen. Av bestämmelsen ska framgå att sådan personuppgiftsbehandling är tillåten om uppgiftslämnandet sker i överensstämmelse med lag eller förordning, dvs. med stöd av bestämmelser som påbjuder eller tillåter utlämnande.

Det närmare innehållet i den föreslagna databasen får regleras på förordnings- och myndighetsföreskriftsnivå.

Vid behandling av personuppgifter som sker för att utföra en uppgift av allmänt intresse, som ett led i myndighetsutövning eller efter en intresseavvägning (dvs. behandling enligt artikel 6.1 e eller 6.1 f i EU:s dataskyddsförordning) ska den registrerade enligt artikel 21.1 i nämnda förordning ha rätt att när som helst, av skäl som hänför sig till hans eller hennes specifika situation, göra invändningar mot behandlingen. Den personuppgiftsansvarige får då inte längre behandla personuppgifterna, såvida denne inte kan påvisa tvingande berättigade skäl för behandlingen som väger tyngre än den registrerades intressen, rättigheter och friheter eller om det sker för fastställande, utövande eller försvar av rättsliga anspråk.

Personuppgifterna i den föreslagna databasen över den statligt tillhandahållna europeiska digitala identitetsplån boken får behandlas med stöd av artikel 6.1 e i EU:s dataskyddsförordning, varför rätten att göra invändningar gäller. Begränsningar av rätten att göra invändningar får enligt artikel 23.1 i förordningen göras i syfte att säkerställa bl.a. ett viktigt mål av generellt allmänt intresse för medlemsstaten. Det krävs också att begränsningen uppfyller krav på nödvändighet och proportionalitet. Vidare måste lagstiftningen enligt artikel 23.2 i förordningen innehålla specifika bestämmelser om bl.a. ändamål, omfattningen av begränsningen, skyddsåtgärder, lagringstid, riskerna för de registrerades rättigheter och friheter samt rätten att bli informerad om begränsningen, när så är relevant.

Regeringen har i tidigare lagstiftningsärende som rör identifiering av fysiska personer framhållit betydelsen av att personuppgifter får behandlas oberoende av den registrerades inställning i de aktuella verksamheterna och att behandlingen är en förutsättning för att myndigheterna ska kunna utföra sina uppgifter på ett korrekt, rättssäkert och effektivt sätt.⁵⁰ I likhet med vad som anfördes i hänvisat lagstiftningsärende kan det förutsättas att den tillhandahållande myndigheten närmast undantagslöst kan påvisa skäl för fortsatt behandling som väger tyngre än den registrerades intressen i det enskilda fallet och att en begränsning av den registrerades rätt att göra invändningar är en proportionerlig åtgärd. Som vi återkommer till i det följande föreslås vissa skyddsåtgärder i samband med nödvändig personuppgiftsbehandling, utöver det integritetsskydd som följer redan av den reviderade eIDAS-förordningen. En bestämmelse om att rätten att göra invändningar inte gäller ska därför föras in i kompletteringslagen. Det finns inte skäl att därutöver införa några ytterligare begränsningar av den registrerades rättigheter.

Personuppgiftsbehandling som utförs i samband med tillhandahållande av uppgifter för personidentifiering

Enligt vårt förslag ska regeringen utse en statlig myndighet som tillhandahållare av uppgifter för personidentifiering (PID) i fråga om fysiska personer. Denna myndighet kommer därmed att behöva behandla personuppgifter. Uppgiftsuppsättningen för PID styrs för närvarande av eIDAS-förordningens genomförandeförordning CIR 2015/1501.⁵¹ De obligatoriska uppgifterna anges i genomförandeförordningens bilaga: a) nuvarande efternamn, b) nuvarande förnamn, c) födelsedatum, d) en unik identitetsbeteckning som satts samman av den utsändande medlemstaten i enlighet med de tekniska specifikationerna för gränsöverskridande identifiering och som är mest beständig i tid. Det är inte fråga om känsliga personuppgifter.

Med beaktande av gällande genomförandeförordning och i likhet med vad som gäller för befintliga svenska e-legitimationer (och enligt förslaget om en statlig e-legitimation) ska i PID ingå person-

⁵⁰ Prop. 2017/18:95 s. 85 f.

⁵¹ Kommissionens genomförandeförordning (EU) 2015/1501 av den 8 september 2015 om interoperabilitetsramverket enligt artikel 12.8 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden.

nummer eller samordningsnummer för personer med styrkt identitet. Som tidigare anförts är vikten av en säker identifiering uppenbar i verksamheten med den europeiska digitala identitetsplånboken. Det finns således stöd för att behandla person- och samordningsnummer utan sådant samtycke som avses i 3 kap. 10 § dataskyddslagen och någon ytterligare bestämmelse om detta behövs inte.

Uppgiften att tillhandahålla PID för koppling till den europeiska digitala identitetsplånboken för fysiska personer ska enligt vårt förslag författningsregleras. Personuppgiftsbehandlingen i samband med utfärdandet av PID kan stödjas på den rättsliga grunden i artikel 6.1 c eller 6.1 e i EU:s dataskyddsförordning. Uppgiften att tillhandahålla en europeisk digital identitetsplånbok är av allmänt intresse, och den personuppgiftsbehandling som uppgiften förutsätter är även nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige. Det är, som redan nämnts, av avgörande betydelse att det går att säkerställa att en fysisk person kan kopplas till en viss europeisk digital identitetsplånbok vid tillhandahållandet, och behandling av personuppgifter i detta avseende är således nödvändig.

Den av regeringen utsedda myndigheten kommer att använda sig av uppgifter om fysiska personers namn och person- respektive samordningsnummer från folkbokföringsdatabasen (eller eventuellt den föreslagna databasen över statliga e-legitimationer). Den uppgiftsöverföring som aktualiseras utgör också en behandling av personuppgifter, för vilken det redan finns (eller föreslås att finnas) laglig grund. Som framgått tillhandahålls redan flera myndigheter uppgifter från Skatteverkets folkbokföringsdatabas (se avsnitt 6.3.3).

När det gäller utfärdande av LPID, dvs. uppgifter för personidentifiering för juridiska personer, innebär vårt förslag att Bolagsverket regeringen ska utse en statlig myndighet för denna uppgift. Ansvaret ska regleras i lag och på förordningsnivå (avsnitt 6.3.3). Den behandling av personuppgifter som kan komma att aktualiseras i den utsedda myndighetens verksamhet med utfärdande av LPID kommer, i likhet med vad som anförts beträffande utfärdande av PID för fysiska personer, att ha stöd i den rättsliga grunden i artikel 6.1 c eller 6.1 e i EU:s dataskyddsförordning.

I huvudsak är det andra uppgifter än personuppgifter som därvid behandlas (företagsnamn och organisationsnummer). Vid utfärdande av LPID kan dock i vissa fall behandling av personuppgifter aktualiseras, eftersom även företagsnamn kan innehålla personuppgifter,

t.ex. ett grundarens alternativt ägarens egennamn.⁵² De personuppgifter som också kommer att bli föremål för behandling i samband med att LPID tillhandahålls är namn på firmatecknare och, eventuellt, dennes kontaktuppgifter för att kontrollera identitet och behörighet att företräda den ifrågasvarande juridiska personen. Det är inte i något fall fråga om känsliga personuppgifter.

Den av regeringen utsedda myndigheten kommer att använda sig av uppgifter om juridiska personers namn och organisationsnummer från befintliga register, bl.a. från det centrala registret över organisationsnummer och aktiebolagsregistret. Den uppgiftsöverföring som kan komma att aktualiseras utgör också en behandling av, i förekommande fall, personuppgifter. De berörda registerförande myndigheterna har, som anförts i det föregående, laglig grund för sådan behandling (se avsnitt 6.3.3).

Mot bakgrund av det anförda görs bedömningen att den behandling av personuppgifter som aktualiseras vid tillhandahållande av sådana uppgifter för personidentifiering som ska kopplas till en europeisk digital identitetsplånbok har stöd i EU:s dataskyddsförordning och inte kräver någon ytterligare nationell författningsåtgärd.

Den reviderade förordningen om elektronisk identifiering är kompatibel med EU:s dataskyddsförordning

Användare av den europeiska digitala identitetsplånboken ska ha full kontroll över hur den används, liksom över vilken information som finns i den. Tillhandahållare av identitetsplånböcker får inte lagra information om användningen som inte är nödvändig för tillhandahållandet av plånbokstjänsterna. De får inte heller kombinera uppgifter för personidentifiering eller några andra personuppgifter som lagras eller som rör användningen av identitetsplånboken med personuppgifter från andra tjänster som erbjuds av tillhandahållaren eller från tredjepartstjänster och som inte krävs för tillhandahållandet av tjänster relaterade till identitetsplånboken (s.k. profilering). Undantag får göras om användaren uttryckligen har begärt att så sker. Personuppgifter som rör tillhandahållandet av digitala identitetsplånböcker

⁵² European Business Register Association (en sammanslutning med europeiska företagsregister, däribland Bolagsverket) anser att juridiska personers företagsnamn som innehåller personnamn på levande personer är personuppgifter enligt definitionen i EU:s dataskyddsförordning och ska behandlas därefter. Jfr EU-domstolen i en dom den 9 november 2010 i målen C-92/09 och C-93/09 ("Schecke").

ska hållas fysiskt och logiskt avskilda från andra data som innehas av utfärdaren av identitetsplånboken (artikel 5a.14 i den reviderade eIDAS-förordningen).

Det tekniska ramverket för identitetsplånboken ska inte tillåta att tillhandahållare av elektroniska attributsintyg eller någon annan part – efter utfärdande av attributsintyget – får del av data som medger spårning, sammankoppling, korrelerande eller att ta del av uppgifter om transaktioner eller användarbeteenden. Undantag kan göras om användaren uttryckligen medgett att så sker. Ramverket ska dock möjliggöra integritetsskyddande teknik som säkerställer avsaknad av kopplingsbarhet när attestering av attribut inte kräver identifiering av användaren (artikel 5a.16). Av förordningen framgår vidare att lösningarna inom det föreskrivna interoperabilitetsramverket är förenliga med reglerna i EU:s dataskyddsförordning (skäl 9).

All behandling av personuppgifter som utförs av medlemsstaterna eller på deras vägnar av organ eller parter som ansvarar för tillhandahållandet av de europeiska digitala identitetsplånböckerna som medel för elektronisk identifiering ska utföras i enlighet med lämpliga och effektiva dataskyddsåtgärder. Behandlingens förenlighet med EU:s dataskyddsförordning ska kunna visas. Den reviderade eIDAS-förordningen hindrar inte medlemsstaterna från att införa nationella bestämmelser för att ytterligare specificera tillämpligheten av sådana åtgärder (artikel 5a.17).

Behov av att överväga bestämmelser som föreskriver vissa andra integritetshöjande åtgärder

Det kan inledningsvis konstateras att vi har övervägt men bedömt att det, för verksamheten med att tillhandahålla den europeiska digitala identitetsplånboken eller att tillhandahålla uppgifter för personidentifiering (PID och LPID), inte är nödvändigt att införa kompletterande bestämmelser om sådana tekniska och organisatoriska åtgärder som avses i artikel 32 i EU:s dataskyddsförordning, såsom exempelvis att begränsa tillgången till personuppgifter. Ifrågavarande ansvar framgår av artikel 24.1 och 25.2 samt av de allmänna principerna för personuppgiftsbehandling i artikel 5.1 f i EU:s dataskyddsförordning. Det följer således direkt av nämnda förordning att tillgången till personuppgifter ska begränsas på olika sätt. Vi bedömer därför att det, för närvarande, inte finns behov av ytterligare reglering i detta avseende

när det gäller tillhandahållande av den europeiska digitala identitetsplån boken.

Den tekniska och säkerhetsrelaterade utvecklingen sker dock i snabb takt och det kan inte uteslutas att ytterligare krav på sådana säkerhetsåtgärder som avses i artikel 32 i EU:s dataskyddsförordning kan komma att behövas. Det finns därmed behov av att möjliggöra att regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare säkerhetsföreskrifter till skydd för personuppgifter.

Utöver detta föreskriftsbemyndigande finns det anledning att reglera följande åtgärder, vilket den reviderade eIDAS-förordningen såväl som EU:s dataskyddsförordning tillåter.

– Sökbegränsning i fråga om uppgifter om lagöverträdelser

Personuppgifter som rör lagöverträdelser kan komma att behandlas i verksamheten med det statliga tillhandahållandet av den europeiska digitala identitetsplån boken, även om det sannolikt inte kommer att aktualiseras i någon större omfattning. Det torde, i sådana fall, handla om ärenden om återkallelse eller spärr av en plån boksinstans utifrån uppgifter som härrör från fällande domar i brottmål eller andra överträdelser. I syfte att undvika sådana integritetsrisker som angiven behandling kan medföra är det lämpligt att i kompletteringslagen införa en sökbegränsning för uppgifter som rör lagöverträdelser.

Uppgifter om lagöverträdelser är inte känsliga personuppgifter men anses ändå vara en typ av uppgifter som förtjänar ett särskilt skydd. I likhet med vad som gäller för person- och samordningsnummer finns stöd för sådan behandling inom ramen för en myndighets verksamhet i artikel 10 i EU:s dataskyddsförordning och 3 kap. 8 § första stycket dataskyddslagen. Det finns därmed, utöver föreslagen sökbegränsning, inte skäl att införa ytterligare bestämmelser om personuppgifter som rör lagöverträdelser.

– En högsta lagringstid för uppgifter i databasen

Vid lagring av personuppgifter som sker helt eller delvis automatiserat eller när personuppgifter ingår i eller kommer att ingå i en databas omfattas behandlingen av EU:s dataskyddsförordnings krav på lagringsminimering. Enligt artikel 5.1 e i dataskyddsförordningen får person-

uppgifter inte lagras på ett sätt som möjliggör identifiering under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas.

Behandling för arkivändamål av allmänt intresse är enligt artikel 5.1 b i EU:s dataskyddsförordning generellt sett laglig, eftersom behandlingen anses vara förenlig med det ändamål för vilket uppgifterna ursprungligen samlades in. Enligt artikel 6.2 och 6.3 i nämnda förordning får medlemsstaterna införa bestämmelser om lagringstider, när behandlingen grundar sig på artikel 6.1 e, vilket vi, som framgått, bedömer är fallet för verksamheten för det statliga tillhandahållandet av den europeiska digitala identitetsplånboken.

Den svenska arkivlagstiftningens utgångspunkt är att allmänna handlingar ska bevaras oavsett huruvida de innehåller personuppgifter. Bestämmelser om bevarande av allmänna handlingar genom arkivering finns i arkivlagen (1990:782), arkivförordningen (1991:446) och Riksarkivets föreskrifter (RA-FS och RA-MS). Den personuppgiftsbehandling som en myndighet utför för att arkivera allmänna handlingar enligt arkivlagstiftningen ska enligt regeringen anses ske för arkivändamål av allmänt intresse i den mening som begreppet har i dataskyddsförordningen. Det skydd som enligt svensk rätt gäller för myndigheters arkiv uppfyller enligt regeringen krav på skyddsåtgärder i EU:s dataskyddsförordning och personuppgifter får därmed bevaras under en längre tid än vad som framgår av principen om lagringsminimering, om den svenska arkivlagstiftningen kräver att uppgifterna ska bevaras.⁵³

I likhet med vad vi anförde beträffande den föreslagna statliga e-legitimationen är det även för det statliga tillhandahållandet av den europeiska digitala identitetsplånboken befogat med en författningsreglerad lagringstid om tio år för uppgifterna i databasen över sådana identitetsplånböcker. Som närmare redovisades i vårt delbetänkande är den föreslagna tidsbegränsningen anpassad efter främst behovet av att kontrollera registrerade uppgifter vid ansökningstillfället för att begränsa risken att samma person innehar flera identitetshandlingar med olika identiteter eller att personen i fråga använder en annan persons identitet.⁵⁴

Regleringen bör ske på förordningsnivå med stöd av ett föreskriftsbemyndigande som införs i kompletteringslagen. Bestämmelsen om

⁵³ Prop. 2017/18:105 s. 110 ff.

⁵⁴ *En säker och tillgänglig digital identitet* (SOU 2023:61), s. 237 ff.

en högsta lagringstid utformas lämpligen på så sätt att uppgifter och handlingar ska gallras senast tio år efter utgången av det kalenderår då det ärende som uppgifterna eller handlingarna hänför sig till avslutades. Ett ärende kan avslutas i samband med att en europeisk digital identitetsplånbok utfärdas, en ansökan avslås eller återkallas eller på annat sätt, exempelvis genom avvísning.

Det behövs ingen särskild författningsreglering för personuppgiftsbehandling som i övrigt sker vid tillhandahållande, användning och återkallelse av europeiska digitala plånböcker

Vid sidan av den myndighet som ska tillhandahålla den europeiska digitala identitetsplånboken och de myndigheter som ska tillhandahålla uppgifter för personidentifiering innebär våra förslag att ytterligare aktörer behöver behandla personuppgifter.

Det är till att börja med fråga om personuppgiftsbehandling som sker hos den myndighet som föreslås ansvara för tillsyn över tillhandahållare av den europeiska digitala identitetsplånboken (se avsnitt 6.6.1). Ifrågavarande uppgift följer direkt av den reviderade eIDAS-förordningen och är därtill av allmänt intresse. Det finns således laglig grund för behandlingen. Vi föreslår att regeringen utser en statlig myndighet för uppgiften och bedömer det lämpligt att PTS, som i dag är tillsynsmyndighet över betrodda tjänster, är ansvarig myndighet även för tillsyn över den europeiska digitala identitetsplånboken. Den personuppgiftsbehandling som sker inom ramen för PTS nuvarande uppdrag är inte särskilt reglerat i den nu gällande kompletteringslagen utan stödjer sig på dataskyddsförordningens bestämmelser. Enligt vår bedömning behövs inte heller för den nu tillkommande tillsynsverksamheten någon särskild reglering i kompletteringslagen.

Tillsynsmyndigheten föreslås vidare ansvara för att i enlighet med artikel 5b i den reviderade eIDAS-förordningen föra ett register över förlitande parter. Även den uppgiften följer direkt av förordningen och får anses vara av allmänt intresse, varför personuppgiftsbehandlingen har laglig grund. Inte heller ifrågavarande behandling av personuppgifter är av sådan omfattning och karaktär att den behöver särskild reglering i nationell rätt.

Som framgått har vi även föreslagit att aktörer inom privat sektor får godkännas som tillhandahållare av den europeiska digitala identitetsplånboken (se avsnitt 6.3.1). Sådana godkända tillhandahållare har

att på eget ansvar uppfylla föreskrivna krav för plånboksfunktioner. Dessa aktörer är även, och i likhet med den tillhandahållande myndigheten, ansvariga för att de uppgifter om användarna som är nödvändiga (och tillåtna) för att tillhandahålla plånbokstjänsterna finns samlade. Utan sådana uppgifter är det exempelvis inte möjligt för en ansvarig tillhandahållare att på användarens begäran återkalla en identitetsplånbok. Dessa tillhandahållare är således också personuppgiftsansvariga för verksamheten och skyldiga att efterleva reglerna om personuppgiftsbehandling i EU:s dataskyddsförordning såväl som bestämmelserna om integritetsskydd som föreskrivs i den reviderade eIDAS-förordningen. Personuppgiftsansvaret innebär bl.a. att tillhandahållare måste ha rättslig grund för sin personuppgiftsbehandling, vilket kan vara andra än de som redovisats i fråga om den tillhandahållande myndigheten. Varje sådan tillhandahållare måste således på egen hand överväga vilken eller vilka rättsliga grunder som nödvändig behandling av personuppgifter kan stödjas på. I den mån sådan personuppgiftsbehandling sker i respektive aktörs verksamhet ankommer det på denne att uppfylla kraven i EU:s dataskyddsförordning.

Slutligen kan anmärkas att de förlitande parter som kommer att agera i förhållande till europeiska digitala identitetsplånböcker, på samma sätt som beskrivits för privata tillhandahållare, är personuppgiftsansvariga för sin respektive verksamhet och är skyldiga att efterleva reglerna om personuppgiftsbehandling i EU:s dataskyddsförordning såväl som bestämmelserna om integritetsskydd som föreskrivs i den reviderade eIDAS-förordningen.

6.3.10 Sekretess

Utredningens förslag: I 6 § offentlighets- och sekretessförordningen (2009:641) ska, bland verksamheter som omfattas av sekretess, tilläggas den databas med uppgifter om den statligt tillhandahållna europeiska digitala identitetsplånboken som den tillhandahållande myndigheten ska föra.

Utredningens bedömning: Några sekretessbrytande bestämmelser behövs inte.

Skälen för utredningens förslag och bedömning

Vårt förslag om det statliga tillhandahållandet den europeiska digitala identitetsplånboken förutsätter personuppgiftsbehandling och att en databas används i den tillhandahållande myndighetens verksamhet för ärendehantering (se avsnitt 6.3.9). Databasen kommer enligt förslaget att innehålla personuppgifter som inte är av känslig art, såsom namn, personnummer alternativt samordningsnummer, och vissa andra uppgifter om exempelvis giltighetstid. I samband med ärendehantering kan dock, om än i begränsad omfattning, även uppgifter om lagöverträdelser komma att behöva behandlas av den tillhandahållande myndigheten. Vi har även föreslagit att personuppgifter får behandlas av den tillhandahållande myndigheten om det är nödvändigt för att fullgöra skyldighet att lämna ut uppgifter till exempelvis andra myndigheter.

Detta föranleder överväganden om behov av uppgiftssekretess.

Att utlämna uppgifter ska ske i överensstämmelse med lag eller förordning. Ett sådant exempel är 6 kap. 5 § offentlighets- och sekretesslagen (2009:400, OSL) som fastslår en allmän skyldighet för en myndighet att på begäran av en annan myndighet lämna ut uppgifter, om det inte skulle hindra arbetets behöriga gång. Av 22 kap. 1 § första stycket OSL följer dock att sekretess gäller för uppgift i verksamhet som avser folkbokföringen eller annan liknande registrering av befolkningen. Sekretessen enligt denna bestämmelse gäller för enskilda personliga förhållanden, om det av särskild anledning kan antas att den enskilde eller någon närstående till denne lider men om uppgiften röjs. Huvudregeln i bestämmelsen är alltså att uppgifterna i de register som avses ska vara offentliga. Om det av särskild anledning kan antas att ett utlämnande skulle leda till skada eller men kan dock uppgifter hemlighållas. Det skulle kunna vara fallet i fråga om uppgifter om lagöverträdelser som kan förekomma i samband med att en tillhandahållen europeisk digital identitetsplånbok har spärrats.

För sådan ”annan verksamhet som avser registrering av en betydande del av befolkningen” som avses i 22 kap. 1 § första stycket OSL får regeringen meddela föreskrifter om sekretess. Exempel på sådana verksamheter är Polismyndighetens passregister och register över nationella identitetskort samt Skatteverkets databas över identitetskort för folkbokförda i Sverige. Detta framgår av 6 § offentlighets- och sekretessförordningen (2009:641). Den verksamhet med statligt till-

handahållna europeiska digitala identitetsplånböcker som nu föreslås är på motsvarande sätt skyddsvärd och bör omfattas av sekretess. Det finns därmed behov av att kunna sekretessskydda sådana uppgifter.

Vi föreslår därför att 6 § offentlighets- och sekretessförordningen ändras med ett tillägg för den verksamhet som avser den tillhandahållande myndighetens databas över den europeiska digitala identitetsplånboken.

I samband med tillhandahållande av den europeiska digitala identitetsplånboken, inbegripet uppgifter för personidentifiering (PID och LPID), kan det bli aktuellt med kontroller mot eller utlämnande av uppgifter från befintliga register som förs av andra myndigheter än de som föreslås att tillhandahålla den europeiska digitala identitetsplånboken respektive PID och LPID. Som anförs i avsnitten 6.3.3 och 6.3.9 är sådan uppgiftshantering möjlig redan i dagsläget och något behov av ytterligare författningsreglering i detta avseende bedöms inte vara nödvändig.

6.4 Gränsöverskridande identitetsmatchning

Utredningens bedömning: Utveckling av en förvaltningsgemensam tjänst för identitetsmatchning – som en del i en nationell digital infrastruktur och som därmed kan minska den administrativa bördan för förlitande parter – är ett arbete som bör främjas. Det är av vikt att framtagna lösningar möter kraven i EU:s reviderade förordning om elektronisk identifiering avseende otvetydig identitetsmatchning i både resultatmässigt och formellt hänseende genom en hög digital gränsöverskridande tillgänglighet till tjänster på såväl hög som låg tillitsnivå.

En sådan förvaltningsgemensam tjänst kan på sikt bidra till Sveriges förmåga att uppfylla kraven om gränsöverskridande identitetsmatchning enligt den reviderade EU-förordningen.

Personuppgifter som kan användas för gränsöverskridande identitetsmatchning omfattas av författningsreglering med hög skyddsnivå.

Skälen för utredningens bedömning

Att stödja användbarheten av e-legitimationer, tillhandahålla bättre offentliga digitala tjänster och öka rättssäkerheten beträffande användarnas elektroniska identitet

Som redovisas i avsnitt 4.6.4 fastställs i artikel 11a.1 i den reviderade eIDAS-förordningen en skyldighet för medlemsstaterna att säkerställa otvetydig identitetsmatchning för fysiska personer som använder anmälda e-legitimationer eller europeiska digitala identitetsplånböcker för gränsöverskridande tjänster. När e-legitimation anges i det följande omfattas även identitetsplånboken och vice versa.

Det nya kravet på identitetsmatchning gäller för medlemsstater i egenskap av förlitande parter, dvs. den träffar offentliga aktörers digitala tjänster. Av artikel 11a.2 framgår också att medlemsstaterna ska föreskriva tekniska och organisatoriska åtgärder för att säkerställa en hög skyddsnivå för personuppgifter som används för identitetsmatchning och för att förhindra profilering av användare. En förteckning över referensstandarder och, vid behov, specifikationer och förfaranden för i artikeln föreskrivna krav ska fastställas i genomförandeakter (artikel 11a.3).

I EU-kommissionens konsekvensbeskrivning av sitt förslag om ”unique identification”, anfördes följande.⁵⁵

[t]he rigid data set for notified eIDs makes it also difficult to match identity records as the current minimum dataset is often not sufficient to uniquely identify a person. Such difficulties typically occur when a person owns different notified eIDs which makes matching the identity to a record difficult using automated means. Problems of identity matching limit the usability of notified eID and is predominantly linked to the cross border use of eIDs since at national level citizens can more easily be identified relying on national identifiers and unique national data sets.

Some service providers require a national registry number to grant access to online public services in order to avoid identity matching problems. However, not all Member states issue such a number and include it in the data set. Obtaining it may require physical presence which is an obstacle for users from abroad even in case they are eligible to obtain a national registry number and to access a service.

⁵⁵ Commission Staff Working Document, Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) n° 910/2014 as regards establishing a framework for a European Digital Identity, 3.6.2021, SWD(2021) 124 final, s. 20.

Several Member States have identified identity matching as a key challenge for the revision of the eIDAS Regulation. Full assurance on record matching / identity matching is a precondition for a seamless cross-border functioning of a European Digital Identity for persons, companies and devices. Without full assurance on identity matching, Member States will be reluctant to open services and agree to an extension of eID/eIDAS to the private sector.

Det är inte klart huruvida dessa formuleringar kan tas till intäkt för satt identitetsmatchning och registermatchning, enligt kommissionen, är att betrakta som synonyma begrepp. Under trilogförhandlingarna förekom ömsom det ena, ömsom det andra, medan den slutliga utformningen av den ifrågasvarande artikeln innehåller enbart identitetsmatchning. Oavsett vilket begrepp som använts har dock formuleringen av dess innebörd enligt definitionen i artikel 3.55 varit i sakens sanna: ”en process där uppgifter för personidentifiering eller medel för elektronisk identifiering matchas mot eller kopplas till ett befintligt konto som tillhör samma person. Detta talar för att det i detta sammanhang är fråga om utbytbara benämningar.⁵⁶

Kravet på gränsöverskridande identitetsmatchning avser att ytterligare stödja användbarheten av e-legitimationer, tillhandahålla bättre offentliga onlinetjänster och öka rättssäkerheten när det gäller användarnas elektroniska identitet (skäl 41).

I dagsläget förutsätts ofta ett svenskt personnummer, eller ett svenskt samordningsnummer, för inloggning i och användning av en digital tjänst som tillhandahålls av en offentlig aktör i Sverige. Sådana identitetsbeteckningar saknas i en utländsk e-legitimation, även när det är fråga om en användare som har ett sådant nummer. Användarens inloggning kan därmed inte kopplas till ärenden och information hos den förlitande parten, dvs. den som kräver inloggning i sin tjänst.

Resultatet blir att personen i fråga hamnar i ett s.k. digitalt väntrum. Det är dock inte bara det nya kravet i den reviderade eIDAS-förordningen som förutsätter en förändring av denna situation. EU:s förordning om en gemensam digital ingång föreskriver bl.a. möjligheten till bevisutbyten och att utföra ärenden online över lands-

⁵⁶ En tolkning som gjorts i Finland, www.eduskunta.fi/SV/vaski/Kirjelma/Sidor/U_41+2021.aspx (hämtad 2024-05-27).

gränser, i förekommande fall efter identifiering med e-legitimation som är anmäld för gränsöverskridande användning.⁵⁷

En svensk tjänst för identitetsmatchning har utretts och utarbetats

Ur ett svenskt perspektiv kan kravet på otvetydig identitetsmatchning medföra att information från en e-legitimation eller europeisk digital identitetsplånbok utfärdad i ett annat EU-land behöver kopplas samman med uppgift om befintligt person- eller samordningsnummer vid inloggning i och användning av en i Sverige tillhandahållen digital tjänst, dvs. en koppling mellan utländska e-legitimationer och svenska identitetsbegrepp. För de fall en sådan koppling görs, på ett sätt som uppfyller kravet på otvetydig identitetsmatchning, genom användning av en förvaltningsgemensam tjänst, kan det finnas förutsättningar för att också återanvända denna koppling när personen i fråga på nytt önskar autentiseras gentemot exempelvis förlitande parter.

Under senare år har arbete utförts av Skatteverket och Digg i syfte att ta fram en förvaltningsgemensam tjänst för identitetsmatchning. I det följande återges myndigheternas respektive redovisning av detta arbete.

Skatteverket

Skatteverket har utrett och i två promemorior redovisat sina överväganden om behoven av och förutsättningarna för en förvaltningsgemensam tjänst för koppling mellan en utländsk e-legitimation och en individs svenska personnummer eller styrkta samordningsnummer vid användning av svenska digitala myndighetstjänster.⁵⁸

⁵⁷ Europaparlamentets och rådets förordning (EU) 2018/1724 av den 2 oktober 2018 om inrättande av en gemensam digital ingång för tillhandahållande av information, förfaranden samt hjälp- och problemlösningstjänster och om ändring av förordning (EU) nr 1024/2012 (Text av betydelse för EES.).

⁵⁸ Uppgifterna är hämtade från promemoriorna *Koppling mellan europeiska eID-handlingar och svenska personnummer eller styrkta samordningsnummer*, 2016-10-24, och *Fördjupad utredning rörande koppling mellan utländska eID-handlingar och svenska identitetsbeteckningar*, 2019-01-21. Beträffande behovsbilden anfördes att för vissa större myndigheter (Pensionsmyndigheten och Skatteverket) finns tydliga behov och stora grupper av möjliga användare, medan behovet inte framstår lika tydligt för andra myndigheter och att viss skepsis råder mot att det går att konstruera en service som är tillräckligt säker för att myndigheterna ska våga använda den.

Skatteverket föreslog till att börja med att myndigheten ska tillhandahålla en kopplingstjänst med ett centralt kopplingsregister.⁵⁹ Genom det centrala registret kan uppgifter om användarens identiteter lagras och behandlas samt kopplingar sparas och förmedlas. Samma grad av säkerhet ska krävas vid registreringen och identifieringen som vid utfärdandet av en fysisk identitetshandling som tillhandahålls av staten, dvs. noggrann identitetskontroll av användaren vid fysisk inställelse hos den identitetskontrollerande myndigheten. Utöver säkerhetsaspekten innebär ett centralt register den fördelen att uppgifterna kommer att finnas tillgängliga för den nationella eIDAS-noden så att användaren av en digital tjänst inte vid varje inloggningstillfälle behöver vänta på att jämförelse ska göras med uppgifter i folkbokföringsdatabasen. Olika lösningar är tänkbara beträffande vilken aktör som gör slagningen mot kopplingsregistret. Myndigheten som har den digitala tjänsten eller Skatteverket skulle kunna utföra slagningen. Med en helt maskinell lösning kan, och bör enligt Skatteverket, funktionen byggas in i den svenska noden, som därför föreslogs ha direktåtkomst till kopplingsregistret för att se hurvida användaren är registrerad. Identitetsbeteckningen skickas till myndigheten som tillhandahåller den digitala tjänsten. Därefter är det den myndigheten som avgör om tillträde ska ges till tjänsten.

Skatteverket har i redovisningen av sitt uppdrag presenterat ytterligare två lösningar som kan utveckla kopplingstjänsten och kopplingsregistret. För det första kan Sverige träffa bi- eller multilaterala avtal med andra länder och enas om att e-legitimationernas unika identitetsbeteckningar ska innehålla personnummer eller motsvarande beständiga identitetsbeteckningar, vilket finns i t.ex. de nordiska länderna. Författningsstöd för att behandla nordiska personnummer i folkbokföringsdatabasen finns redan (2 kap. 3 § 16 lagen om behandling av personuppgifter i Skatteverkets folkbokföringsverksamhet). Bestämmelsen kan på sikt utökas med identitetsbeteckningar från andra medlemsstater. För det andra finns inget som hindrar att en användare kan ha flera e-legitimationer utfärdade i olika länder. En digital väg att registrera en koppling till en utländsk e-legitimation är att användaren själv kan göra en e-legitimationskoppling. Det innebär att användaren loggar in med en tidigare kopplad e-legitimation och godkänner

⁵⁹ Förslaget utesluter inte att en myndighet kan använda en (egen) kopplingstjänst utan ett centralt register, om tillitsnivå 2 enligt det svenska tillitsramverket för e-legitimationer räcker för den myndighetens digitala tjänster. Nödvändiga uppgifter för en sådan koppling finns tillgängliga via Navet.

att ytterligare en utländsk e-legitimation kopplas till den svenska identitetsbeteckningen (id-växling). Detta ger en möjlighet till registrering med motsvarande säkerhetsnivå som vid fysisk inställelse.

Skatteverkets förslag har inte genomförts.

Digg

Under senare tid har säkerställande av identitetsmatchning ingått som en del i ett regeringsuppdrag för Digg. Myndigheten har konstaterat att Sverige behöver säkerställa vissa grundförmågor:

1. Förmåga till gränsöverskridande identitetsmatchning mellan en utländsk e-legitimation och ett befintligt svenskt identitetsbegrepp för en fysisk person.
2. Förmåga att hantera beständig koppling mellan en utländsk e-legitimation och ett svenskt identitetsbegrepp.
3. Förmåga att utfärda ett svenskt identitetsbegrepp för EU/EES-medborgare som saknar relation till Sverige.⁶⁰

Dessa grundförmågor kan realiseras på olika sätt som myndighets-specifika eller förvaltningsgemensamma funktioner och tjänster med tillhörande fördelar och nackdelar. Förmågan enligt punkten 1 är baserad på de personuppgifter som medföljer vid användning av en utländsk e-legitimation som genomgått anmälningsförfarandet för gränsöverskridande användning enligt eIDAS-förordningen (artiklarna 7 och 9) och eventuella ytterligare attribut (utan formell tillitsnivå) som användaren själv kan tillföra inom ett förfarande (dvs. digital tjänst).⁶¹ Förmågan enligt andra punkten avser att kunna registrera, lagra och återanvända en gjord koppling mellan en utländsk e-legitimation och ett svenskt identitetsbegrepp. Detta kan i grunden jämföras med Skatteverkets ovan redovisade förslag om kopplingsregister. Syftet med en sådan koppling är att den ska vara tillförlitlig och beständig över viss tid för att ge användaren återkommande behörighet till bl.a. digitala tjänster i Sverige ”på samma tillitsnivå som en svensk e-legitimation som utfärdas för samma person och samma identitets-

⁶⁰ Myndigheten för digital förvaltning, *Genomförandeplan för införandet av bevisutbyte enligt engångsprincipen*, 2021–12–15, *Analys och förslag på gemensamma lösningar* (bilaga 2) s. 10.

⁶¹ Myndigheten för digital förvaltning, a.a. s. 12 ff.

begrepp”.⁶² Beträffande förmågan enligt tredje punkten konstaterades ett behov av att kunna tilldela ett svenskt identitetsbegrepp (liknande samordningsnummer) helt online till användare som identifierar sig i ett svenskt onlineförfarande med en utländsk e-legitimation som anmälts i enlighet med eIDAS-förordningen. Syftet skulle vara att uppnå samma spårbarhet kring dessa individers kontakter med Sverige som för övriga icke folkbokförda individer som använder ett svenskt identitetsbegrepp som samordningsnummer.⁶³

I redovisningen av uppdraget *föreslog* Digg bl.a. en förvaltningsgemensam tjänst för identitetsmatchning som ska tillhandahållas online av lämplig myndighet, t.ex. Skatteverket, samt även utvecklas som öppen källkod för att kunna göras tillgänglig för myndigheter som kan ha särskilda motiverade behov av att förvalta myndighets-specifika lösningar baserade på samma källkod. Vidare rekommenderades fortsatt analys kring dels behov och möjligheter att hantera beständiga kopplingar mellan utländska e-legitimationer och svenska identitetsbegrepp, dels behov och möjligheter på kort och lång sikt att utfärda ett svenskt identitetsbegrepp helt eller delvis online till personer, som använder svenska digitala tjänster via gränsöverskridande identifiering i enlighet med eIDAS-förordningen, utan tidigare relation till Sverige.⁶⁴

Sedan slutredovisningen av myndighetsuppdraget driver Digg ett projekt i vilket en förvaltningsgemensam tjänst för identitetsmatchning utvecklas inom ramen för Diggs ansvar enligt EU:s förordning om en gemensam digital ingång. Det är upp till varje förlitande part att välja att använda Diggs lösning eller att utveckla en egen.⁶⁵ Enligt uppgift från företrädare för Digg bedöms tjänsten kunna tas i bruk tidigast i början av år 2025.

⁶² Myndigheten för digital förvaltning, a.a. s. 15.

⁶³ Ibid. Det har via underhandskontakter med företrädare för myndigheten framkommit att det även finns behov att säkerställa behovet av en förmåga att stödja svenska medborgare med behov av att identifiera sig mot andra länders digitala tjänster. Det handlar om att kunna förmedla de identitetsbegrepp dessa länder behöver för att genomföra en identitetsmatchning mot sina identitetsbegrepp.

⁶⁴ Myndigheten för digital förvaltning, a.a. s. 28.

⁶⁵ www.digg.se/digitala-tjanster/identitetsmatchning (hämtad 2024-05-27).

Fortsatt arbete på området behövs

Det uppställda kravet avseende gränsöverskridande identitetsmatchning innebär att offentliga förlitande parter ska ha förmåga att säkerställa otvetydig identitetsmatchning av en användare vid varje användningstillfälle. Att utarbeta en förvaltningsgemensam matchningstjänst föreskrivs inte uttryckligen i den reviderade eIDAS-förordningen, men det torde bidra till Sveriges förmåga att uppfylla förordningens krav i detta.

Det finns beröringspunkter mellan eIDAS-förordningen och EU:s förordning om en gemensam digital ingång, och de utmaningar som förordningarnas krav föranleder är delvis gemensamma. Inrättandet av den europeiska digitala identitetsplånboken har skapat förhoppningar om att problem kopplade till den gränsöverskridande användningen av e-legitimationer och svårigheter att uppfylla vissa krav enligt EU:s förordning om en gemensam digital ingång ska kunna minska. Med identitetsplånbokens funktioner att lagra och hantera elektroniska attributsintyg förväntas förutsättningarna för identitetsmatchning (och bevisutbyten enligt EU:s förordning om en gemensam digital ingång) att förbättras. Även eventuellt kommande genomförandakter med reviderad reglering av den obligatoriska uppgiftsuppsättningen för e-legitimationer kan antas omfatta ytterligare attribut, och även fler frivilliga sådana attribut.⁶⁶ Det medför att uppgiftssammansättningen torde bli mer användbar för elektronisk identifiering.

En användare med koppling till Sverige, men vars europeiska digitala identitetsplånbok tillhandahållits av en annan medlemsstat, skulle exempelvis kunna lagra ett elektroniskt attributsintyg avseende matchad svensk identitet, att presentera för bl.a. förlitande parter. Identitetsplånbokens funktionalitet medför att en separat tjänst inte i och för sig är nödvändig för att visa en matchad identitet vid användning av digitala tjänster.

En identitetsmatchningstjänst kan dock ändå behövas, särskilt för att tillgodose matchningsbehov för användare som saknar identitetsplånbok.

Utvecklande av en förvaltningsgemensam tjänst för identitetsmatchning är således alltså ett arbete som behövs, och bör främjas.

⁶⁶ För närvarande regleras detta i Kommissionens genomförandeförordning (EU) 2015/1501 av den 8 september 2015 om interoperabilitetsramverket enligt artikel 12.8 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden, och i bilagan till förordningen.

En sådan tjänst kan bidra till en nationell digital infrastruktur och därmed minska den administrativa bördan för förlitande parter. Det är av vikt att framtagna lösningar möter den reviderade eIDAS-förordningens krav på otvetydig identitetsmatchning i både resultatmässigt och formellt hänseende genom en hög digital gränsöverskridande tillgänglighet till tjänster på såväl hög som låg tillitsnivå.

Givet att sådana infrastrukturella lösningar täcker behovet för majoriteten av användare och förlitande parter i samhället kan, som nämnts, en gemensam tjänst också bidra till Sveriges förmåga att på sikt uppfylla kraven om gränsöverskridande identitetsmatchning enligt den reviderade eIDAS-förordningen.

Tilläggs kan att det, till skillnad från när Skatteverket redovisade sitt förslag, nu finns tekniska lösningar motsvarande inskanning och läsning av exempelvis pass för att koppla identiteten på en högre tillitsnivå.⁶⁷

Som nämns ovan ska medlemsstaterna föreskriva tekniska och organisatoriska åtgärder för att säkerställa en hög skyddsnivå för personuppgifter som används för identitetsmatchning. De personuppgifter som i första hand är aktuella att användas för identitetsmatchning finns i folkbokföringsdatabasen.⁶⁸ För helt eller delvis automatiserad eller på annat sätt strukturerad behandling av personuppgifter i folkbokföringsverksamheten gäller primärt EU:s dataskyddsförordning och de särskilda dataskyddsbestämmelserna i lagen om behandling av personuppgifter i Skatteverkets folkbokföringsverksamhet och förordningen (2001:589) om behandling av personuppgifter i Skatteverkets folkbokföringsverksamhet. Personuppgifterna omfattas av författningsreglering med hög skyddsnivå. Redan av EU:s dataskyddsförordning följer att profilering av användare är otillåten (artikel 22). Det bör dock i det nödvändiga fortsatta arbetet på detta område utredas om detta skydd är tillräckligt för att uppfylla det uppställda kravet i den reviderade eIDAS-förordningen om att skydda personuppgifter som kan användas för identitetsmatchning.

⁶⁷ Se t.ex. Migrationsverkets pilotprojekt med distansvisningar av originalhandlingar, www.migrationsverket.se/Om-Migrationsverket/Pressrum/Nyhetsarkiv/Nyhetsarkiv-2024/2024-05-16-Arbetstagare-och-studenter-kan-visa-pass-for-Migrationsverket-i-mobiltelefonen.html (hämtad 2024-05-27).

⁶⁸ Användning av biometriska uppgifter och passavläsning, vilket skulle kunna aktualiseras vid en distansmatchning på högre tillitsnivå är föremål för utredning, dir. 2023:134 *Utökade befogenheter för Skatteverket inom brottbekämpning och folkbokföring*.

6.5 Betrodda tjänster

6.5.1 Allmänt om bedömning av överensstämmelse

Utredningens förslag: Den nuvarande 2 § andra stycket i lagen med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering och 2 § i förordningen med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering ska upphävas.

Utredningens bedömning: Det behövs ingen kompletterande nationell reglering av överensstämmelse, kontrollformer och rapportering.

Skälen för utredningens förslag och bedömning

I den ursprungliga eIDAS-förordningen ställs det krav på bedömning av överensstämmelse för tillhandahållare av betrodda tjänster som vill ha status som kvalificerad och de betrodda tjänster som de vill ska vara kvalificerade. I den reviderade eIDAS-förordningen ställs utöver de krav som sedan tidigare fanns på betrodda tjänster numera krav på att europeiska digitala identitetsplånböcker och anmälda system för elektronisk identifiering ska genomgå bedömning av överensstämmelse i enlighet med artikel 5c respektive artikel 12a.⁶⁹ Vidare har det i artikel 45f.3 lagts till en bestämmelse om bedömning av överensstämmelse för tillhandahållare av elektroniska intyg på attribut utfärdade av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa.

Enligt artikel 3.18 i den reviderade eIDAS-förordningen definieras ett organ för bedömning av överensstämmelse som ett organ som omfattas av definitionen i artikel 2.13 i förordning (EG) nr 765/2008. Det betyder att ett sådant organ i enlighet med förordningen om ackreditering är ackrediterat som behörigt för att utföra bedömning av överensstämmelse av en kvalificerad tillhandahållare av en betrodd tjänst och den kvalificerade betrodda tjänst som denne tillhandahåller, eller som behörigt att utföra certifiering av europeiska digitala identi-

⁶⁹ Enligt artikel 20 jämförd med artikel 3.18 i eIDAS-förordningen ska kvalificerade tillhandahållare av betrodda tjänster minst en gång vartannat år granskas av ett organ för bedömning av överensstämmelse som är ackrediterat enligt Europaparlamentets och rådets förordning (EG) nr 765/2008.

tetsplånböcker eller medel för elektronisk identifiering. Ackreditering enligt förordning (EG) nr 765/2008 innebär att ett nationellt ackrediteringsorgan förklarar att ett organ för bedömning av överensstämmelse uppfyller kraven i harmoniserade standarder och, i förekommande fall, ytterligare krav.

I Sverige är Styrelsen för ackreditering och teknisk kontroll (Swedac) nationellt ackrediteringsorgan. Ett organ som vill bli ackrediterat måste lämna en ansökan till Swedac som prövar och bedömer om organet uppfyller de krav som ställs i förordning (EG) nr 765/2008, lagen (2011:791) om ackreditering och teknisk kontroll med tillhörande förordning samt föreskrifter som Swedac har meddelat. Organet måste också uppfylla de sektorsspecifika krav som organet ska arbeta i enlighet med. Ackreditering beviljas i form av ett ackrediteringsintyg som gäller för viss tid eller tills vidare och som innehåller de villkor som gäller för ackrediteringen. Det följer av eIDAS-förordningen att ackreditering av organ för bedömning av överensstämmelse ska ske enligt förordning (EG) nr 765/2008. Kompletterande bestämmelser till den förordningen finns i lagen om ackreditering och teknisk kontroll.

Lagen gäller i princip all ackreditering som Swedac utför, oavsett om den föreskrivs i förordning (EG) nr 765/2008 eller sker på annan grund. I och med att den reviderade eIDAS-förordningen anger att organen för bedömning av överensstämmelse ska vara ackrediterade enligt förordning (EG) nr 765/2008 finns det därför inget behov av att i den kompletterande lagen till den reviderade eIDAS-förordningen ange att ackreditering ska ske på det sättet. Den reviderade eIDAS-förordningen innehåller inte några bestämmelser om hur ackrediteringen ska gå till, t.ex. när det gäller vilken kontrollform som ska användas eller vilka krav som organen för bedömning av överensstämmelse ska uppfylla. Detta kommer dock förtydligas genom att kommissionen enligt artikel 20.4 senast den 21 maj 2025 i genomförandeakter ska upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för ackreditering av organ för bedömning av överensstämmelse och för rapport om bedömning av överensstämmelse. Genomförandeakten ska även omfatta granskningskrav för hur organ för bedömning av överensstämmelse ska göra sin bedömning, inbegripet sammansatt bedömning, vad gäller kvalificerade tillhandahållare av betrodda tjänster.

Eftersom det kommer att finnas krav på dessa områden i genomförandeakter finns inte längre ett behov av nationell reglering och bemyndiganden att föreskriva om specifika krav för ackrediteringen eller rapporteringen av certifieringen som finns i lagen respektive förordningen med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering. Den nuvarande föreskriftsrätten har inte heller nyttjats av PTS under den tiden bemyndigandet har funnits. Dessa bestämmelser ska därför upphävas.

6.5.2 Krav på certifiering av betrodda tjänster

Utredningens bedömning: Det behövs inga nya eller ändrade nationella kompletterande bestämmelser vad gäller bedömning av överensstämmelse av betrodda tjänster.

Skälen för utredningens bedömning

Kraven på bedömning av överensstämmelse är i stort sett samma i den reviderade eIDAS-förordningen som i den tidigare gällande eIDAS-förordningen. Den förändring som skett är att delar av säkerhetskraven för icke-kvalificerade och kvalificerade tillhandahållare av betrodda tjänster⁷⁰ nu ställs via det s.k. NIS2-direktivets artikel 21 med tillhörande genomförandeakt.⁷¹ NIS2-reglerna kommer att behöva omfattas i den bedömning av överensstämmelse som ett ackrediterat organ för bedömning av överensstämmelse ska göra av en tillhandahållare av betrodda tjänster och de betrodda tjänster denne vill ska vara certifierade i enlighet med artikel 20 i eIDAS-förordningen.

Den andra nyheten är att den nya betrodda tjänsten elektroniskt attributsintyg utfärdat av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa, som definieras i artikel 3.46 i den reviderade eIDAS-förordningen, omfattas av krav på bedömning av överensstämmelse. Kraven liknar i allt väsentligt kraven på kvalificerade tillhandahållare av betrodda tjänster, men kravet på bedömning av överensstämmelse följer direkt av kraven i artikel 45f.7 där EU-kom-

⁷⁰ Kraven ställdes tidigare i eIDAS-förordningens artikel 19.

⁷¹ Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS2-direktivet).

missionen, senast den 21 november 2024, genom genomförandeakter ska upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för tillämpningen av tjänsten och överensstämmelsebedömning för tjänsten. Dessa genomförandeakter ska vara förenliga med de genomförandeakter som avses i artikel 5a.23 om genomförandet av den europeiska digitala identitetsplånboken. Flera av de organ som i dag är ackrediterade för bedömning av överensstämmelse för kvalificerade tillhandahållare och betrodda tjänster i enlighet med eIDAS-förordningen blir troligtvis organ för bedömning av överensstämmelse även för denna nya betrodda tjänst.

Enligt artikel 45f.3 i den reviderade eIDAS-förordningen ska medlemsstaterna underrätta kommissionen om de offentliga organ som avses i artikel 3.46. Det saknas behov av någon särskild reglering för att tillse att denna underrättelseskyldighet fullgörs.

Ingen av de ovan nämnda förändringarna medför ett behov av nya eller ändrade nationella regler. Det påverkar inte heller ansvarsförhållanden mellan myndigheter på annat sätt än att det kommer finnas ett ökat behov av samarbete mellan ansvariga myndigheter för tillsyn av betrodda tjänster enligt eIDAS-förordningen respektive NIS2-direktivet när det direktivet har genomförts i svensk lagstiftning.

6.5.3 Krav på certifiering av anordningar

Utredningens förslag: Regeringen eller den myndighet som regeringen bestämmer ska utse ansvarigt organ för certifiering av anordningar för skapande av kvalificerade elektroniska underskrifter och anordningar för skapande av kvalificerade elektroniska stämplor.

Den nuvarande 3 § i lagen med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering och 3 § i förordningen med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering ska upphävas.

Bestämmelsen i 5 § andra stycket förordningen (2007:854) med instruktion för Försvarets materielverk ska upphävas.

Utredningens bedömning: Certifieringsorgan som är ackrediterade enligt cybersäkerhetsakten är bäst lämpade att genomföra certifiering av anordningar för skapande av kvalificerade underskrifter och anordningar för skapande av kvalificerade elektroniska stämplor.

Skälen för utredningens förslag och bedömning

I den reviderade eIDAS-förordningen ställs i huvudsak samma krav på anordningar för skapande av kvalificerade elektroniska underskrifter och stämplat som tidigare. Det finns emellertid två förändringar mot vad som tidigare gällt. Den första förändringen är att de certifikat som utfärdats efter certifieringen är tidsbestämda, men kan förlängas i enlighet med artikel 30.3a i den reviderade förordningen. Den andra förändringen är att det blivit en betrodd tjänst i sig att tillhandahålla en anordning för skapande av kvalificerade underskrifter eller stämplat på distans i enlighet med artikel 29a i den reviderade förordningen.

Inte heller bestämmelserna om vem som certifierar anordningar för kvalificerade elektroniska underskrifter och stämplat har ändrats. Bestämmelserna återfinns i artiklarna 30 och 39 i den ursprungliga eIDAS-förordningen. Enligt artikel 30.1 ska medlemsstaterna utse lämpliga privata eller offentliga organ som ska certifiera anordningar för skapande av kvalificerade elektroniska underskrifter och med stöd av artikel 39 gäller artikel 30 även stämplat. Av artikel 30.2 följer att medlemsstaterna ska underrätta EU-kommissionen om vilket organ som utsetts. I Sverige är CSEC certifieringsorgan och uppgiften regleras i 5 § andra stycket förordningen (2007:854) med instruktion för Försvarets materielverk. Enligt 3 § lagen med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering, får regeringen eller den myndighet som regeringen bestämmer meddela föreskrifter om certifiering för anordningar för skapande av kvalificerade elektroniska underskrifter och stämplat. Enligt 3 § förordningen med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering, får PTS meddela föreskrifter om certifiering om anordningar med undantag för säkerhetsegenskaper. Enligt andra stycket i samma paragraf får MSB meddela föreskrifter om säkerhetsegenskaper som dessa förordningar ska uppfylla. Ingen av myndigheterna har använt bemyndigandena att meddela föreskrifter. Efter ett genomförandebeslut från 2016 finns inte heller något behov av bemyndigandena.⁷²

⁷² Kommissionens genomförandebeslut (EU) 2016/650 av den 25 april 2016 om fastställande av standarder för säkerhetsbedömning av kvalificerade anordningar för skapande av elektroniska underskrifter och stämplat enligt artiklarna 30.3 och 39.2 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden.

Även om eIDAS-förordningens bestämmelser avseende nu aktuell certifiering inte har ändrats har det däremot skett förändringar i regelverket kring certifiering (se mer om detta i avsnitt 6.3.7). Dessa ändringar innebär att den certifiering som CSEC har som uppgift att göra inte längre får utföras efter den 27 februari 2026. Mot denna bakgrund måste nuvarande certifieringsordning ses över för att Sverige ska uppfylla kravet i artiklarna 30 och 39 i eIDAS-förordningen. Detta innebär även att bestämmelsen i 5 § andra stycket förordningen med instruktion för Försvarets materielverk ska upphävas.

I fråga om vilka organ som är lämpliga att utföra certifiering av anordningar för skapande av kvalificerade elektroniska underskrifter och stämplars bedömer vi i likhet med den bedömning som görs i avsnitt 6.3.7, att de certifieringsorgan som är ackrediterade enligt cybersäkerhetsakten är bäst lämpade för denna uppgift. Artikel 30 anger därtill att både statliga och privata organ kan utses. Någon begränsning vad gäller att organet måste vara svenskt kan inte heller anses föreligga. Det går emellertid inte, med den osäkerhet som nu råder (se mer om detta i avsnitt 6.3.7), att närmare peka ut vilket eller vilka organ som skulle utfärda de nödvändiga certifieringarna. Ett bemyndigande om att regeringen, eller den myndighet som regeringen bestämmer, ska få utse ett organ för certifiering av anordningar för skapande av kvalificerade elektroniska underskrifter och stämplars ska därför tas in i kompletteringslagen. Ansvarig myndighet ska framgå av kompletteringsförordningen.

Vi bedömer att FMV som nationell myndighet för cybersäkerhetscertifiering är bäst lämpad att utse ett sådant organ. Formerna för hur ett sådant organ utses kan variera beroende på de förutsättningar som råder, t.ex. om det krävs att FMV initierar ett upphandlingsförfarande. I ett scenario där det saknas möjlighet att utse ett ackrediterat certifieringsorgan i antingen Sverige eller något annat EU-land kan FMV även i teorin utse att myndigheten på egen hand ska utföra certifieringen. Ett sådant utfall framstår emellertid som mindre troligt.

6.6 Ett styrningsramverk för tillsyn och samarbete

I den reviderade eIDAS-förordningens kapitel IVa regleras de funktioner som gemensamt utgör vad som kallas ett styrningsramverk. Detta omfattar, utöver tillsyn över det så kallade ramverket för den

europiska digitala identitetsplånboken samt över betrodda tjänster, även funktioner för samarbete och ömsesidigt bistånd. Nedan följer våra förslag och bedömningar kopplade till de åtgärder som medlemsstaterna ska vidta inom ramen för styrningsramverket.

6.6.1 Tillsyn över den europeiska digitala identitetsplånboken

Utredningens förslag: Den myndighet regeringen bestämmer ska utöva tillsyn över att sådana tillhandahållare av europeiska digitala identitetsplånböcker som är etablerade i Sverige efterlever dels kraven i EU:s reviderade förordning om elektronisk identifiering och de rättsakter som har meddelats med stöd av förordningen, dels kraven i lagen med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering och de föreskrifter som har meddelats med stöd av densamma.

Tillsynsmyndigheten ska

- ha rätt att på begäran få de upplysningar och handlingar som behövs för tillsynen samt ha rätt att få tillträde till områden, lokaler och andra utrymmen, förutom bostäder, där verksamhet bedrivs,
- ha rätt att få biträde av Kronofogdemyndigheten för tillsynen,
- få meddela de förelägganden och förbud som behövs för tillsynen och
- få bestämma att dess beslut ska gälla omedelbart.

Regeringen, eller efter regeringens bemyndigande, tillsynsmyndigheten, ska få meddela föreskrifter om skyldighet för tillhandahållare av den europeiska digitala identitetsplånboken att betala avgift för tillsynsmyndighetens verksamhet.

Utredningens bedömning: Post- och telestyrelsen är den myndighet som är bäst lämpad att utöva tillsyn över europeiska digitala identitetsplånböcker och tillhandahållare av sådana identitetsplånböcker.

Skälen för utredningens förslag och bedömning

Tillsynsorganets roll och uppgifter

Varje medlemsstat ska utse ett eller flera tillsynsorgan som är etablerade på dess territorium. Tillsynsorganet ska ges nödvändiga befogenheter och tillräckliga resurser för att kunna utföra sin uppgift på ett ändamålsenligt, effektivt och oberoende sätt (artikel 46a.1).

Tillsynsorganets roll ska vara att utöva tillsyn över tillhandahållare av europeiska digitala identitetsplånböcker etablerade i den medlemsstat där de har utsetts och – genom tillsynsverksamhet på förhand och i efterhand – säkerställa att såväl tillhandahållare av som de utfärdade identitetsplånböckerna uppfyller kraven i förordningen. Uppdraget ska också omfatta att vid behov vidta åtgärder med avseende på tillhandahållare av identitetsplånböcker genom tillsynsverksamhet i efterhand om tillsynsmyndigheten informeras om att bestämmelserna i förordningen åsidosätts av tillhandahållarna eller av tillhandahållna identitetsplånböcker (artikel 46a.3 a och 46a.3 b).

I förordningen anges vidare vilka uppgifter som särskilt ska inbegripas i tillsynsorganets verksamhet. Däribland finns att samarbeta med och bistå andra tillsynsorgan, begära nödvändig information för att övervaka efterlevnaden av förordningen samt informera relevanta myndigheter och den gemensamma kontaktpunkten om säkerhetsincidenter eller integritetsförluster i vissa angivna fall. Vidare ingår att utföra inspektioner på plats och utöva tillsyn på distans samt kräva att tillhandahållare av europeiska digitala identitetsplånböcker åtgärdar varje underlåtenhet att uppfylla kraven i förordningen (se artikel 46a.4 a–e och 46a.4 g). Tillsynsmyndigheten ska också enligt artikel 46a.4 f, vid olaglig eller bedräglig användning av den europeiska digitala identitetsplånboken, tillfälligt eller permanent upphäva registreringen och inkluderingen av förlitande parter i den mekanism som avses i artikel 5b.7 (se mer om detta i avsnitt 6.6.2).

Om tillsynsorganet, med stöd av artikel 46a.4 e, har krävt att en tillhandahållare av en europeisk digital identitetsplånbok åtgärdar en underlåtenhet att uppfylla kraven enligt förordningen, och tillhandahållaren inte agerar i enlighet med detta samt – i tillämpliga fall, inom en tidsfrist som fastställts av tillsynsorganet – får tillsynsorganet ålägga tillhandahållaren att tillfälligt eller permanent upphöra med tillhandahållandet av den europeiska digitala identitetsplånboken (se avsnitt 6.3.1). Tillsynsorganet ska i angivet fall utan onödigt dröjs-

mål informera tillsynsorganen i övriga medlemsstater, kommissionen, förlitande parter och användare av den europeiska digitala identitetsplån boken om beslutet att kräva att tillhandahållandet av den europeiska digitala identitetsplån boken tillfälligt eller permanent upphör (se artikel 46a.5).

I huvudsak motsvarande bestämmelser ska gälla för tillsyn över den europeiska digitala identitetsplån boken som för tillsyn över betrodda tjänster

Enligt 5 § kompletteringslagen gäller att tillsynsmyndigheten över betrodda tjänster har rätt att på begäran få de upplysningar och handlingar som behövs för tillsynen samt att få tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, där det bedrivs verksamhet som står under tillsyn. Vid behov har myndigheten rätt att få biträde av Kronofogdemyndigheten vid sin tillsyn. Av 6 § samma lag framgår vidare att tillsynsmyndigheten får meddela de förelägganden och förbud som behövs för efterlevnaden av dels förordningen, dels lagen eller av föreskrifter som meddelats med stöd av den. Förelägganden och förbud får förenas med vite och tillsynsmyndigheten får bestämma att besluten ska gälla omedelbart.

Regeringen konstaterade vid kompletteringslagens tillkomst att det var en uppgift för tillsynsmyndigheten att utforma en lämplig tillsynsverksamhet med utgångspunkt från de uppgifter som framgick av eIDAS-förordningen, och att en grundläggande förutsättning för en fungerande tillsyn är att tillsynsmyndighetens initiativ och beslut är väl underbyggda. Enligt regeringen var det därför viktigt att tillsynsmyndigheten kunde få tillgång till de upplysningar och handlingar som bedömts nödvändiga för tillsynen, samt vid behov få tillträde där verksamhet som omfattas av förordningen bedrivs. På så sätt kunde upprätthållande av en effektiv tillsynsverksamhet säkerställas. Regeringen ansåg också att tillsynsmyndigheten, när den upptäcker brister i en verksamhet, bör kunna utfärda de förelägganden eller förbud som behövs för att rättelse ska ske. Förordningens krav på att det ska finnas effektiva, proportionella och avskräckande sanktioner motiverade därmed att förelägganden och förbud skulle få förenas med vite.⁷³

⁷³ Se prop. 2015/16:72 s. 48 f.

Enligt vår bedömning gör sig motsvarande skäl, med undantag för möjligheten att förena förelägganden och förbud med vite (se vidare nedan), gällande för tillsyn över den europeiska digitala identitetsplånboken som för tillsyn över betrodda tjänster. Vi menar därför att bestämmelsen om tillsyn över identitetsplånboken, med angivet undantag, bör motsvara vad som gäller för betrodda tjänster enligt 4–6 §§ kompletteringslagen.

Den reviderade förordningen bedöms inte medge vitessanktion för tillsyn över identitetsplånböcker

Den reviderade förordningen föreskriver i artikel 16 – på samma sätt som tidigare – att medlemsstaterna ska fastställa bestämmelser om effektiva, proportionella och avskräckande sanktioner som ska gälla vid överträdelser av förordningen. Som ovan redovisats var det angiven bestämmelse som enligt regeringen motiverade att förelägganden och förbud som meddelas av tillsynsmyndigheten för betrodda tjänster skulle få förenas med vite.

Vi har övervägt om artikel 16 eller någon annan bestämmelse i förordningen motiverar införande av en motsvarande vitessanktion för överträdelser vid tillhandahållande av en europeisk digital identitetsplånbok och gjort följande bedömning.

Det kan inledningsvis konstateras att artikel 16 i dess helhet är underordnad förordningens tredje kapitel som behandlar just betrodda tjänster, vilket i sig motiverar slutsatsen att artikeln är avsedd att gälla endast sådana tjänster. Ordalydelsen av artikelns första punkt, jämfört med dess andra, inger emellertid visst tvivel. Artikel 16.1 anger nämligen att ”medlemsstaterna ska fastställa bestämmelser om sanktioner som ska gälla vid *överträdelser av denna förordning*”. Artikel 16.2 anger i stället att ”medlemsstaterna ska säkerställa att överträdelser av denna förordning *som begås av kvalificerade och icke-kvalificerade tillhandahållare av betrodda tjänster* medför administrativa sanktionsavgifter”. Det kan således konstateras att artikel 16.1, till skillnad från artikel 16.2 i och för sig inte utesluter att den är tillämplig på andra överträdelser än sådana som avser betrodda tjänster.

Tillsynen över identitetsplånböcker regleras som framgått i artikel 46a medan den över betrodda tjänster regleras i artikel 46b. Regleringen är i flera avseenden samstämmig. Det framgår exempelvis att de båda tillsynsmyndigheterna har rätt att kräva åtgärdande av varje

underlåtenhet att uppfylla kraven i förordningen av de likalydande bestämmelserna i artiklarna 46a.4 e respektive 46b.4 j.

När det gäller möjligheten att vidta åtgärder till följd av underlåtenhet att uppfylla förordningens krav skiljer sig emellertid bestämmelserna åt. Av artikel 46a.5, som gäller identitetsplånböckerna, framgår att tillsynsorganet – om en tillhandahållare av en europeisk digital identitetsplånbok inte agerar i enlighet med ett av tillsynsmyndigheten utfärdat föreläggande – får ålägga tillhandahållaren att tillfälligt eller permanent upphöra med tillhandahållandet av den europeiska digitala identitetsplånboken. Någon motsvarande bestämmelse finns inte i artikel 46b, som gäller tillsyn över betrodda tjänster. En åtskillnad av handlingsutrymmet i fråga om tillsynen avseende betrodda tjänster respektive identitetsplånböcker tycks således vara avsedd, vilket får sägas vara förenligt med att handlingsutrymmet för överträdelser av regelverket för betrodda tjänster i stället framgår av artikel 16. En tolkning som utsträcker artikel 16 till att reglera sanktioner för den europeiska digitala identitetsplånboken framstår mot angiven bakgrund som alltför långtgående. En annan sak är att en europeisk digital identitetsplånbok kan innehålla betrodda tjänster som omfattas av bestämmelserna i artikel 16.

Det redovisade leder oss till bedömningen att avsikten är att den enda påföljden vid underlåtenhet att efterfölja tillsynsmyndighetens över europeiska digitala identitetsplånböcker krav på åtgärdande är att tillhandahållaren ska upphöra med sin verksamhet. Vi föreslår därför inte att förbud och förelägganden ska få förenas med vite.

Vi vill dock framhålla att ett så ingripande påtryckningsmedel som upphörande – som enda remedium – riskerar att leda till icke önskvärda effekter. Vi anser att detta medför en risk för större acceptans för missförhållanden eftersom konsekvenserna av att ett tillhandahållande upphör blir omfattande både för enskilda och för olika funktioner i samhället. Att kunna tillgripa en vitessanktion innan ett beslut om upphörande skulle enligt vår bedömning kunna utgöra ett effektivt sätt att motverka missförhållanden utan att ett stort antal användare blir av med sin europeiska digitala identitetsplånbok. Om kommande genomförandeakter medger utrymme för en sådan sanktion anser vi att det bör övervägas.

Tillsynsmyndigheten ska ha rätt att ta ut en avgift

Även om full kostnadstäckning inte kommer att uppnås framstår det, på samma sätt som för tillsyn över tillhandahållare av betrodda tjänster, som naturligt att låta tillsynsmyndighetens över den europeiska digitala identitetsplån boken verksamhet delvis finansieras av dem som berörs av verksamheten och för dem som har nytta av den.⁷⁴ Närmare bestämmelser om avgiftssystemets utformning kan meddelas med stöd av föreslaget bemyndigande som tas in i kompletteringslagen.

Tillsynsmyndighetens beslut ska få gälla omedelbart

Åtgärder som vidtas med digitala identitetsplån böcker sker direkt och kan avse betydande ekonomiska värden samt integritetskänsliga uppgifter. Om brister i tillhandahållandet av de digitala identitetsplån böckerna upptäcks är det därför av avgörande betydelse att tillsynsmyndigheten skyndsamt kan ingripa. Tillsynsmyndigheten bör därför ha möjlighet att bestämma att dess beslut ska gälla omedelbart.

Post- och telestyrelsen är bäst lämpad att vara tillsynsmyndighet

PTS har i dag till uppgift att vara tillsynsmyndighet enligt kompletteringslagen och ge stöd och information till myndigheter och enskilda när det gäller betrodda tjänster. Myndigheten har därutöver ytterligare tillsynsansvar, bl.a. enligt lagen (2010:751) om betaltjänster och enligt lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.⁷⁵ Således har PTS redan i dag tillsynsansvar över verksamheter som har ett naturligt samband med den europeiska digitala identitetsplån boken och besitter därmed för uppdraget värdefull kunskap och erfarenhet. Vidare kan tillsyn för betydande delar av digitaliseringsområdet samlas om det är PTS som ges ansvar även för tillsyn över europeiska digitala identitetsplån böcker. Vi bedömer att ett samlat tillsynsansvar medför samordningsvinster som i sin tur kan förväntas leda till ökad kostnadseffektivitet när det gäller tillsyn på digitaliseringsområdet. Enligt vår bedömning föreligger inga rollkonflikter eller

⁷⁴ Se prop. 2015/16:72 s. 54 f. och där gjorda hänvisningar.

⁷⁵ Se 4 § 14 p och 21 p samt 6 b § förordning (2007:951) med instruktion för Post- och telestyrelsen.

andra intressekonflikter som skulle hindra att PTS ges ifrågavarande tillsynsansvar.

Vi har övervägt om någon annan myndighet skulle kunna vara lämplig att utöva tillsyn över europeiska digitala identitetsplånböcker. I vårt delbetänkande framhöll vi att Digg i och för sig skulle kunna utöva tillsyn över e-legitimationer. Därmed skulle Digg också kunna utöva tillsyn över den europeiska digitala identitetsplånboken. Eftersom vi nu bedömer att Digg ska utfärda den europeiska digitala identitetsplånboken är det emellertid inte en lämplig ordning.⁷⁶ Några ytterligare myndigheter som skulle vara lämpliga har vi inte kunnat identifiera.

6.6.2 Tillsynsmyndigheten ska ansvara för registret över förlitande parter

Utredningens förslag: Tillsynsmyndigheten över europeiska digitala identitetsplånböcker ska ansvara för att upprätta, underhålla och offentliggöra ett register över förlitande parter som förlitar sig på de europeiska digitala identitetsplånböckerna.

Skälen för utredningens förslag

Förlitande parter ska registrera sig

En förlitande part som avser att förlita sig på europeiska digitala identitetsplånböcker för tillhandahållande av offentliga eller privata tjänster genom digital interaktion ska registrera sig i den medlemsstat där den är etablerad (artikel 5b.1).

Registreringen av förlitande parter ska enligt förordningen underlätta medlemsstaternas kontroller av lagenligheten hos de förlitande parternas verksamhet i enlighet med unionsrätten och syfta till att öka öppenheten i och förtroendet för användningen av europeiska digitala identitetsplånböcker. Registreringen ska vara kostnadseffektiv och stå i proportion till riskerna för att säkerställa att den sprids bland tjänsteleverantörerna. I förordningens ingress anges att registreringen i detta sammanhang bör innebära att automatiserade förfaranden används, inbegripet att medlemsstaterna förlitar sig på och använder

⁷⁶ Jfr *En säker och tillgänglig statlig e-legitimation* (SOU 2023:61), s. 180 ff.

befintliga register, och den bör inte innefatta något förfarande för förhandsgodkännande (se skäl 17).

Vid registreringen ska den förlitande parten åtminstone ange den information som krävs för autentisering till europeiska digitala identitetsplånböcker. Sådan information omfattar enligt förordningen i vart fall den medlemsstat där den förlitande parten är etablerad och den förlitande partens namn samt, i tillämpliga fall, dess registreringsnummer i enlighet med vad som framgår i ett officiellt register, tillsammans med identifieringsuppgifter från samma register. Vidare ska kontaktuppgifter till den förlitande parten, liksom den avsedda användningen av europeiska digitala identitetsplånböcker – inbegripet angivande av de uppgifter som den förlitande parten ska begära från användare – anges (se artikel 5b.2). Den förlitande parten får sedan inte begära att en användare tillhandahåller några andra uppgifter än dem som angetts och ska utan dröjsmål informera medlemsstaten vid eventuella ändringar (artikel 5b.3 och 5b.6).

Medlemsstaten ska göra den information som en förlitande part tillhandahåller tillgänglig för allmänheten online i elektroniskt under-tecknad eller stämplad form som lämpar sig för automatiserad behandling (se artikel 5b5).

Tillsynsmyndigheten ska ansvara för registret över förlitande parter

Utöver det som redovisats i avsnitt 6.6.1 innefattar tillsynsmyndighetens uppgifter enligt artikel 46a.4 f i den reviderade förordningen att – vid olaglig eller bedräglig användning av den digitala identitetsplånboken – tillfälligt eller permanent upphäva registreringen och inkluderingen av förlitande parter i den mekanism som, enligt artikel 5b.7, ska inrättas för att möjliggöra identifiering och autentisering av förlitande parter.

Artikel 5b.7 föreskriver att medlemsstaten ska tillhandahålla en gemensam mekanism för att möjliggöra identifiering och autentisering av förlitande parter, enligt vad som avses i artikel 5a.5 c. Av artikel 5a.5 c framgår att europeiska digitala identitetsplånböcker ska säkerställa att förlitande parter kan autentiseras och identifieras genom att autentiseringsmekanismer genomförs i enlighet med artikel 5b. Som framgått föreskriver artikel 5b i sin tur att det ska finnas ett register över förlitande parter.

Vi har mot angiven bakgrund uppfattat att tillsynsansvaret över den europeiska digitala identitetsplånboken och registret över förlitande parter är avsett att hänga samman. Vi föreslår därför att tillsynsmyndigheten ska ansvara för registret över förlitande parter. Vi har bedömt att PTS är den myndighet som är bäst lämpad att utöva tillsyn över europeiska digitala identitetsplånböcker (se avsnitt 6.6.1). PTS är i dagsläget inte en registerförande myndighet varför etablering av de strukturer som krävs kommer att vara kostnadsdrivande för myndigheten (se avsnitt 8.7).

Redovisade bestämmelser omfattas av kommande genomförandeförordningar, vilka kan komma att medge en annan tolkning av sambandet mellan tillsynsmyndigheten och registret över förlitande parter. I sådant fall finns det anledning att överväga om en mer kostnadseffektiv lösning skulle vara att en myndighet som i dagsläget har de strukturer som krävs för att tillhandahålla registret i stället bör ges detta ansvar.

Artikel 46a.4 f innehåller som framgått en uttrycklig bestämmelse som ger tillsynsorganet rätt att tillfälligt eller permanent upphäva registreringen och inkluderingen av förlitande parter i den mekanism som avses i artikel 5b.7 vid olaglig eller bedräglig användning av den europeiska digitala identitetsplånboken. En särskild bestämmelse som medger tillsynsmyndigheten en sådan möjlighet behöver således inte införas i lagen.

Någon närmare beskrivning av hur tillsynsmyndigheten, som inte har något egentligt tillsynsansvar över förlitande parter, får lov att agera för att tillgodogöra sig erforderligt underlag inför sitt beslut att upphäva registreringen och inkluderingen av förlitande parter framgår inte av förordningen. Det framhålls dock att det är av stor betydelse för att säkerställa förtroendet för, och en bred spridning av, europeiska digitala identitetsplånböcker att unionsmedborgare och invånare i unionen skyddas mot obehörig eller bedräglig användning av identitetsplånböckerna. Det poängteras vidare att tillsynsorganet – särskilt om en nationell rättslig myndighet i något annat förfarande fastställt fakta som utgör bedräglig eller annan olaglig användning – efter anmälan bör vidta nödvändiga åtgärder. Åtgärderna anges syfta till att säkerställa att registreringen av den förlitande parten och inkluderingen av förlitande parter i autentiseringsmekanismen återkallas eller tillfälligt upphävs till dess att den anmälande myndigheten bekräftar att de konstaterade oriktigheterna har åtgärdats (se skäl 18 i förordningens ingress).

Kommissionen ska fastställa tekniska specifikationer och förfaranden för angivna mekanismer i kommande genomförandeakter. Om dessa medför behov av ytterligare nationella bestämmelser är i dagsläget inte möjligt att avgöra. Vi bedömer därför att det för närvarande inte krävs några nationella bestämmelser såvitt avser hanteringen av registret utöver den nu föreslagna om vilken myndighet som ska ansvara för registret.

6.6.3 Tillsynsmyndigheten ska agera vid säkerhetsincidenter

Utredningens förslag: Vid säkerhetsincidenter som rör europeiska digitala identitetsplånböcker, valideringsmekanismer eller det system för elektronisk identifiering inom ramen för vilket sådana identitetsplånböcker tillhandahålls, ska tillsynsmyndigheten (över europeiska digitala identitetsplånböcker) vidta åtgärder i enlighet med artikel 5e.1–3 i EU:s reviderade förordning om elektronisk identifiering.

Utredningens bedömning: Post- och telestyrelsen är lämpad att ansvara för att vidta åtgärder vid säkerhetsincidenter som rör europeiska digitala identitetsplånböcker.

Skälen för utredningens förslag och bedömning

Tillhandahållandet och användningen av identitetsplånböcker ska tillfälligt upphävas eller återkallas vid säkerhetsincidenter

Vi har i avsnitt 6.3.1 ovan redovisat förordningens, i artikel 5a.9, krav på att identitetsplånbokens giltighet omedelbart ska kunna återkallas i vissa angivna fall. Bestämmelsen behandlar enligt vårt förmenande möjligheten att återkalla en specifik plånboksinstans, alltså en viss fysisk eller juridisk persons identitetsplånbok.

Återkallelse av en viss plånbokslösning behandlas i stället i artikel 5e. Av bestämmelsens första punkt följer att i de fall europeiska digitala identitetsplånböcker som tillhandahålls i enlighet med artikel 5a, de valideringsmekanismer som avses i artikel 5a.8, eller det system för elektronisk identifiering inom ramen för vilket de europeiska digitala identitetsplånböckerna tillhandahålls – är föremål för incidenter eller

delvis äventyras på ett sätt som påverkar deras tillförlitlighet, eller tillförlitligheten för andra europeiska digitala identitetsplånböcker – ska den medlemsstat som tillhandahöll de europeiska digitala identitetsplånböckerna utan onödigt dröjsmål tillfälligt upphäva tillhandahållandet och användningen av europeiska digitala identitetsplånböcker.

När det är motiverat mot bakgrund av allvaret i ifrågavarande säkerhetsincident eller äventyrande ska medlemsstaten återkalla europeiska digitala identitetsplånböcker utan onödigt dröjsmål (artikel 5e.1 andra stycket).

Om den säkerhetsincident eller det äventyrande som avses i punkt 1 första stycket i artikel 5e inte åtgärdas inom tre månader från det tillfälliga upphävandet, ska den medlemsstat som tillhandahöll de europeiska digitala identitetsplånböckerna återkalla de europeiska digitala identitetsplånböckerna och upphäva deras giltighet. Medlemsstaten ska informera de berörda användarna, de gemensamma kontaktpunkter som utsetts i enlighet med artikel 46c.1, de förlitande parterna och kommissionen om återkallandet (artikel 5e.2). I motsatt fall ska tillhandahållandet och användningen i stället återupprättas (artikel 5e.3).

Tillsynsmyndigheten ska uppdras att vidta föreskrivna åtgärder

Uppgiften att vid säkerhetsincidenter tillfälligt upphäva eller återkalla tillhandahållandet av plånbokslösningar enligt artikel 5e ska enligt vår bedömning utföras av den myndighet som utövar tillsyn över identitetsplånböckerna (inbegripet ifrågavarande valideringsmekanismer) och systemen för elektronisk identifiering. På så sätt skapas ett sammanhållet system utan onödiga informationsförluster som riskerar att försena sådana nödvändiga åtgärder som vid säkerhetsbrister måste vidtas mycket skyndsamt. Eftersom tillsynsmyndigheten enligt våra förslag också ska utses till gemensam kontaktpunkt enligt artikel 46c.1 (se mer i avsnitt 6.6.4) kan även den informationsskyldighet som föreskrivs i artikel 5e genomföras utan onödigt dröjsmål.

6.6.4 Tillsynsmyndigheten ska ha vissa ytterligare uppgifter

Utredningens förslag: Tillsynsmyndigheten över europeiska digitala identitetsplånböcker ska utgöra gemensam kontaktpunkt för betrodda tjänster, europeiska digitala identitetsplånböcker och anmälda system för elektronisk identifiering enligt artikel 46c i EU:s reviderade förordning om elektronisk identifiering.

För att uppfylla förordningens krav enligt artikel 46d.2 andra stycket, om att medlemsstaten ska besluta om samt inrätta arrangemang och förfaranden för gemensamma åtgärder för ömsesidigt bistånd, ska tillsynsmyndigheten ges rätt att meddela föreskrifter.

Skälen för utredningens förslag

Tillsynsmyndigheten är central i styrningsramverket

Styrningsramverket omfattar utöver tillsynsansvar även funktioner för samverkan. I artikel 46c föreskrivs till att börja med att varje medlemsstat ska utse en gemensam kontaktpunkt för betrodda tjänster, europeiska digitala identitetsplånböcker och anmälda system för elektronisk identifiering. Den gemensamma kontaktpunkten ska utöva en sambandsfunktion för att underlätta gränsöverskridande samarbete mellan tillsynsorganen för tillhandahållare av betrodda tjänster och mellan tillsynsorganen för tillhandahållare av europeiska digitala identitetsplånböcker samt, när det är lämpligt, med kommissionen och Europeiska unionens cybersäkerhetsbyrå (Enisa), liksom med andra behöriga myndigheter i sin medlemsstat (artikel 46c.1 och 46c.2). Varje medlemsstat ska enligt artikel 46c.3 offentliggöra och utan onödigt dröjsmål meddela kommissionen namnen på och adresserna till den gemensamma kontaktpunkten och eventuella senare ändringar av denna. Kommissionen ska därefter offentliggöra en förteckning över den gemensamma kontaktpunkt som utsetts (artikel 46c.4).

I artikel 46d föreskrivs att de tillsynsorgan som utsetts enligt artikel 46a.1 och 46b.1 – för att underlätta tillsynen och efterlevnaden av skyldigheterna enligt förordningen – får söka ömsesidigt bistånd från tillsynsorganen i andra medlemsstater (bl.a. genom den samsamarbetsgrupp för digital identitet som ska inrättas enligt artikel 46e.1 se nedan). De berörda medlemsstaterna ska i enlighet med sin nationella rätt besluta om och inrätta arrangemangen och förfarandena för

de gemensamma åtgärder som ska vidtas inom ramen för det ömsesidiga biståndet (artikel 46d.2 andra stycket).

Vi bedömer att de funktioner som ska inrättas antingen har en direkt koppling till tillsynsmyndighetens uppgifter eller får anses vara en naturlig del av dess verksamhetsområde. Mot den bakgrunden – och eftersom det bidrar till ett sammanhållet ansvar – föreslår vi att tillsynsmyndigheten utses till gemensam kontaktpunkt. För att uppfylla förordningens krav om att medlemsstaterna, i enlighet med sin nationella rätt, ska besluta om samt inrätta arrangemangen och förfarandena för gemensamma åtgärder i anslutning till det ömsesidiga biståndet ska tillsynsmyndigheten ges rätt att meddela föreskrifter.

Nämnda samarbetsgrupp för digital identitet ska enligt vad som anges i förordningen inrättas av kommissionen för att stödja och underlätta medlemsstaternas gränsöverskridande samarbete och informationsutbyte om betrodda tjänster, europeiska digitala identitetsplånböcker och anmälda system för elektronisk identifiering (artikel 46e.1). Samarbetsgruppen ska bestå av företrädare som utnämns av medlemsstaterna och av kommissionen samt ledas av kommissionen. Medlemsstaterna ska säkerställa att deras utsedda företrädare samarbetar på ett effektivt och ändamålsenligt sätt i samarbetsgruppen (artikel 46e.2 och 6). Vi anser att bestämmelsen utifrån dess lydelse och innehåll, till skillnad från 46c och 46d, inte förutsätter nationell författningsreglering. Det bör emellertid ankomma på tillsynsmyndigheten att utse ifrågavarande representant.

Också det rapporteringskrav som följer av artikel 48a i den reviderade eIDAS-förordningen bör tillgodoses av tillsynsmyndigheten men förutsätter inte författningsreglering.

6.6.5 Tillsyn över betrodda tjänster

Utredningens bedömning: Det behövs inga nya eller ändrade bestämmelser om tillsyn över betrodda tjänster.

Skälen för utredningens bedömning

Den främsta skillnaden som finns mellan den reviderade eIDAS-förordningen och den ursprungliga vad gäller tillsynen av betrodda tjänster är att denna reglering flyttats från avsnittet betrodda tjänster till det

nya avsnittet styrningsramverket, (artikel 46b). Det har även lagts till en skyldighet för tillsynsmyndigheten enligt den reviderade eIDAS-förordningen att informera tillsynsmyndigheten som ansvarar för sektorn som omfattar betrodda tjänster enligt NIS2-direktivet om inträffade säkerhetsincidenter enligt artikel 46b.4 a. De materiella bestämmelserna om tillsyn har dock inte ändrats. Något behov av nya eller ändrade bestämmelser i svensk rätt bedöms därför inte vara nödvändig när det gäller själva tillsynen. Vi föreslår emellertid att nya bestämmelser om administrativa sanktionsavgifter ska tas in i kompletteringslagen (se avsnitt 6.6.7).

6.6.6 Tillsynsstrukturen för nationellt utfärdade e-legitimationer behöver ses över

Utredningens bedömning: Det finns behov av en mer omfattande tillsynsstruktur över e-legitimationer i Sverige. Hur en sådan tillsyn ska vara utformad bör utredas i särskild ordning.

Skälen för utredningens bedömning

I vårt delbetänkande konstaterade vi att utfärdare av e-legitimationer i Sverige står under enbart begränsad tillsyn. Den tillsyn som finns är uppdelad på flera statliga myndigheter och kan kortfattat beskrivas enligt följande.

PTS är ansvarig tillsynsmyndighet för betrodda tjänster som omfattar BankID när tjänsten används för att skapa elektroniska underskrifter. PTS får, liksom Digg och MSB, även meddela föreskrifter kopplat till eIDAS-förordningen och kompletteringslagen (vi föreslår emellertid att denna föreskriftsrätt tas bort vad gäller PTS och MSB, se avsnitt 6.5.1 och 6.5.3). Digg förvaltar och utvecklar tillitsramverket för kvalitetsmärket Svensk e-legitimation samt granskar om e-legitimationsutfärdare uppfyller kraven i tillitsramverket och därmed får använda sig av kvalitetsmärket. Det finns emellertid inga sanktionsmöjligheter kopplade till tillitsramverket och utfärdares efterlevnad av detsamma. Varken Digg eller MSB har alltså något tillsynsansvar kopplat till eIDAS-förordningen eller till nationellt utfärdade e-legitimationer.

Vidare omfattas viss del av Finansiell ID-teknik BID AB:s (som ger ut BankID) verksamhet av säkerhetsskyddslagen (2018:585) för vilken Länsstyrelsen i Stockholm rapporterar säkerhetsskyddsincidenter till Säkerhetspolisen.

Slutligen kan Finansiell ID-teknik BID AB anses vara ett sådant företag som ska kunna bedriva verksamhet i händelse av en fredstida krisituation eller vid höjd beredskap och därmed ska delta i Riksbankens beredskapsplanering.⁷⁷

I delbetänkandet redovisade vi att bristen på tillsyn var otillfredsställande, men gjorde bedömningen att en mer omfattande översyn av tillsynsstrukturen på e-legitimationsområdet låg utanför vårt uppdrag i den delen.⁷⁸

Behovet av en tydligare tillsynsstruktur och mer samverkan har även framhållits i flera andra utredningar. Betalningsutredningen konstaterade exempelvis att det finns en risk att tillsynen blir mindre effektiv när den är utspridd på flera myndigheter än om den hade varit mer centraliserad. Den utredningen antog att den reviderade eIDAS-förordningen skulle komma att påverka ansvarsfördelningen mellan myndigheterna och rekommenderade regeringen att invänta förhandlingarna, samt därefter genomföra en översyn av tillsynsansvaret för e-legitimationer och betrodda tjänster i syfte att uppnå en mer samlad, tydlig och ändamålsenlig tillsynsstruktur kring e-legitimationer och dess utgivare.⁷⁹ Behovet av ökad tillsyn på e-legitimationsområdet i Sverige framhålls vidare av flera remissinstanser som yttrat sig över vårt delbetänkande.⁸⁰

Att lämna förslag om tillsyn över e-legitimationer som utfärdas i Sverige omfattas inte heller i denna del av vårt uppdrag. Vi har emellertid kunnat konstatera att kraven i den reviderade förordningen kan sägas förutsätta att det finns en tydlig tillsynsstruktur på hela e-legitimationsområdet. Skälet till det är att en förutsättning för att kunna skaffa en europeisk digital identitetsplånbok är att användaren först har tillgång till en e-legitimation. Att identitetsplånboken då, men inte de e-legitimationer som används för att skaffa en sådan, står under tillsyn riskerar att påverka säkerheten i infrastrukturen i dess helhet.

⁷⁷ Se *En ny riksbankslag – Volym 1* (SOU 2019:46), s. 1805.

⁷⁸ *En säker och tillgänglig statlig e-legitimation* (SOU 2023:61), s. 181 f.

⁷⁹ *Staten och betalningarna, Del 1*, (SOU 2023:16), s. 380 ff.

⁸⁰ Se exempelvis Bolagsverkets remissvar 2024-01-30 (dnr AD 5259/2023), Finansinspektionens remissvar 2024-01-24, (dnr 23-29976) och Totalförsvarets forskningsinstitutets remissvar 2024-01-22 (dnr FOI-2023-1892).

Att tillsynskravet inte skulle omfatta alla e-legitimationer som utfärdas i Sverige framstår således som bristfälligt av säkerhetsskäl. Eftersom identitetsplån boken i sig är ett medel för elektronisk identifiering (se avsnitt 6.3.1) – vilken alltså står under tillsyn enligt eIDAS-förordningen – framstår det också som en brist ur ett konkurrensperspektiv.

Det är angeläget att skyndsamt genomföra en översyn av tillsynsstrukturen över e-legitimationsområdet för att säkerställa att utfärdade e-legitimationer – även efter godkännande enligt tillitsramverkets regler – möter erforderliga säkerhetskrav. Vi har därför övervägt möjligheten att föreslå att tillsynsmyndigheten över den europeiska digitala identitetsplån boken ska utöva tillsyn också över nationellt utfärdade e-legitimationer. Vi bedömer emellertid att ett sådant förslag, inom ramen för vårt uppdrag, inte är möjligt att lämna eftersom det i dag saknas ett tydligt författningsstöd för en tillsynsmyndighet att förhålla sig till. Hur tillsynen och ifrågavarande författningsstöd ska vara utformat bör i stället utredas i särskild ordning.

6.6.7 Bestämmelser om administrativa sanktionsavgifter ska införas i kompletteringslagen

Utredningens förslag: Bestämmelser om administrativa sanktionsavgifter ska tas in i lagen med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

Tillsynsmyndigheten över betrodda tjänster ska besluta om sanktionsavgift.

Skälen för utredningens förslag

I eIDAS-förordningens artikel 16 finns sedan tidigare krav på att medlemsstaterna ska fastställa bestämmelser om sanktioner som ska tillämpas vid överträdelse av förordningen såvitt avser regelverket för betrodda tjänster.⁸¹ Sanktionerna ska enligt förordningen vara effektiva, proportionerliga och avskräckande. Bestämmelser om tillsynsmyndighetens över betrodda tjänster rätt till administrativa ingripanden genom att kräva åtgärdande av underlåtenhet att upprätthålla

⁸¹ Vi har gjort bedömningen att föreskrivna sanktioner avser endast betrodda tjänster, se mer i avsnitt 6.6.1.

förordningens krav och återkalla en tillhandahållares status som kvalificerad regleras i förordningen, medan rätt att meddela behövliga förelägganden och förbud har införts i kompletteringslagen. Förelägganden och förbud får förenas med vite.⁸² Den reviderade eIDAS-förordningen föranleder inga förändringar i angivna avseenden (se avsnitt 6.6.5).

Regeringen ansåg vid införandet av kompletteringslagen att det då saknades underlag för ytterligare sanktioner utöver att förelägganden och förbud skulle få förenas med vite. Enligt regeringen innehöll kraven på tillhandahållare av betrodna tjänster i artikel 19–24 i eIDAS-förordningen i stor utsträckning bedömningsmoment och lämplighetsöverväganden som gjorde att överträdelser av förordningens bestämmelser ofta kunde vara svåra att konstatera och kräva omfattande utredning. Regeringen bedömde därför att överträdelser av bestämmelserna lämpade sig mindre väl för ett system med sanktionsavgifter.⁸³

Också den reviderade eIDAS-förordningen innehåller i artikel 16.1, med i allt väsentligt samma lydelse som tidigare, en bestämmelse som föreskriver att medlemsstaterna ska fastställa bestämmelser om effektiva, proportionerliga och avskräckande sanktioner. Därutöver föreskrivs nu i artikelns andra punkt att medlemsstaterna ska säkerställa att överträdelser av förordningen som begås av kvalificerade och icke-kvalificerade tillhandahållare av betrodna tjänster ska medföra maximala administrativa sanktionsavgifter på minst a) 5 000 000 EUR om tillhandahållaren av betrodna tjänster är en fysisk person, eller b) om tillhandahållaren av betrodna tjänster är en juridisk person 5 000 000 EUR eller 1 procent av den totala globala årsomsättningen för det företag som tillhandahållaren av betrodna tjänster tillhörde under det räkenskapsår som föregick det år då överträdelsen inträffade, beroende på vilket som är högst.

Således finns det nu krav om inrättande av administrativa sanktionsavgifter i förordningen. Några uttryckliga bestämmelser om hur sanktionsavgifterna bör utformas utöver den nyss redovisade innehåller den reviderade förordningen inte. Bestämmelserna om sanktionsavgifter omfattas inte heller av kommande genomförandeakter.

⁸² 4–6 §§ i lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering jämte artikel 17.4 j och 20.3 i förordningens ursprungliga lydelse.

⁸³ Se prop. 2015/16:72 s. 48.

En sanktionsavgift är en administrativ åtgärd som riktar sig mot en konstaterad överträdelse av en författningsbestämmelse. Det är fråga om en ingripande åtgärd och det krävs att förfarandet är förutsägbart samt möter krav på rimlig handläggningstid, domstolsprövning och en rättssäker process. I likhet med vad som gäller inom andra rättsområden föreslår vi därför att bestämmelser om sanktionsavgifter ska tas in i lag. Bestämmelserna behöver vara mer utförliga än den befintliga regleringen i kompletteringslagen rörande administrativa ingripanden och det ska framgå av lagen när, hur och av vem sanktionsavgift får tas ut.⁸⁴

Den reviderade eIDAS-förordningen lämnar utrymme för att välja domstol eller tillsynsmyndighet för beslut om sanktionsavgift (se artikel 16.3).

I svensk nationell rätt anses en tillsynsmyndighet generellt vara lämpad att besluta om sanktionsavgift när reglerna är relativt enkla att tillämpa, beslutsfattandet är förhållandevis schabloniserat och sanktionsbestämmelserna bygger på strikt ansvar. Om det är aktuellt att pröva subjektiva rekvisit eller andra svårbedömda rekvisit anses ofta en domstol vara mer lämpad. En fördel med att tillsynsmyndigheten fattar beslut har i tidigare lagstiftningsärenden angetts vara att handläggningen blir snabbare eftersom inte flera myndigheter måste involveras i hanteringen.⁸⁵

Tillsynsmyndigheten över betrodda tjänster får förväntas förvärva en särskild kunskap om de verksamheter som ska granskas. Regelverket kring betrodda tjänster innefattar därtill flertalet komplexa frågor som kräver sakkunskap, vilket tillsynsmyndigheten kan förväntas inneha. Vi anser därför att myndigheten bör ha goda förutsättningar att upptäcka och bedöma överträdelser av bestämmelserna i förordningen.⁸⁶ Enligt våra förslag ska sanktionsbestämmelserna också bygga på strikt ansvar och vara förhållandevis utförligt reglerade i lag vilket ytterligare talar för att tillsynsmyndigheten är lämpad att besluta om sanktionsavgifter. Föreslagen ordning gäller dessutom på ett flertal motsvarande områden.⁸⁷

⁸⁴ Jfr t.ex. prop. 2017/18:232 s. 317 ff. och Kammarrätten i Jönköpings dom den 22 november 2017 i mål nr 1847-16.

⁸⁵ Se t.ex. prop. 2017/18:205 s. 68.

⁸⁶ Jfr *Vad bör straffas* (SOU 2013:38), s. 545 f.

⁸⁷ Se exempelvis 29 § lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Med hänsyn till det anförda bör det vara tillsynsmyndigheten över betrodda tjänster, och inte domstol, som bestämmer om sanktionsavgift ska tas ut i det enskilda fallet och hur hög avgiften i så fall ska vara. Besluten kommer emellertid i enlighet med 8 § kompletteringslagen kunna överklagas till allmän förvaltningsdomstol (se mer om överklagande i avsnitt 6.7).

6.6.8 Överträdelser som ska leda till sanktionsavgift

Utredningens förslag: Tillsynsmyndigheten över betrodda tjänster får ta ut sanktionsavgift av kvalificerade och icke-kvalificerade tillhandahållare av betrodda tjänster som:

1. utger sig för att vara en kvalificerad tillhandahållare utan att vara det, eller tillhandahåller en icke-kvalificerad betrodd tjänst som utges vara kvalificerad,
2. har lämnat oriktiga eller ofullständiga uppgifter vid ansökan om att bli kvalificerad,
3. innehar status som kvalificerad tillhandahållare av betrodda tjänster eller har en kvalificerad betrodd tjänst, och inte i enlighet med artikel 24.2 a i EU:s reviderade förordning om elektronisk identifiering informerar om någon ändring av tillhandahållandet av tjänsten eller en avsikt att upphöra med verksamheten,
4. missbrukar EU-förtroendemärket för kvalificerade betrodda tjänster,
5. underlåter att rapportera om sådana incidenter som ska rapporteras enligt artikel 19a.1 b och artikel 24.2 fb i EU:s reviderade förordning om elektronisk identifiering,
6. överträder ett beslut av tillsynsmyndigheten om föreläggande som innebär ett förbud.

Skälen för utredningens förslag

Utgångspunkter

Som ovan redovisats innehåller den reviderade förordningen, utöver lägsta maximala avgifter, inga uttryckliga bestämmelser om hur sanktionsavgifterna ska utformas. I förordningens ingress anges emellertid att medlemsstaterna bör fastställa regler om sanktioner för överträdelser, såsom direkta eller indirekta metoder som leder till förväxling mellan icke-kvalificerade och kvalificerade betrodda tjänster eller till att icke-kvalificerade tillhandahållare av betrodda tjänster missbrukar EU-förtroendemärket (se skäl 45).

Flertalet aktörer som är tillhandahållare av betrodda tjänster är vinstdrivande företag som verkar i konkurrens. Regelverket behöver därför utformas på ett sätt som ger aktörerna incitament att följa kraven som ställs upp. Utgångspunkterna vid övervägande av vilka överträdelser som ska medföra sanktionsavgift bör vara syftet med aktuell bestämmelse och vikten av att den efterlevs. För att kravet på förutsägbarhet ska kunna upprätthållas bör emellertid endast sådana överträdelser som tydligt kan avgränsas och som inte kräver ett alltför stort mått av tolkning kunna omfattas av sanktionsavgift. Det finns ett antal principiellt viktiga regler i både den ursprungliga och reviderade eIDAS-förordningen som enligt vår bedömning vid bristande efterlevnad ska kunna medföra att tillsynsmyndigheten tar ut en sanktionsavgift.

Tillhandahållaren utger sig för att vara kvalificerad tillhandahållare av betrodd tjänst eller tillhandahåller en icke-kvalificerad betrodd tjänst som utges vara kvalificerad

Förordningen reglerar bl.a. tillit till betrodda tjänster och den högsta tilliten ska finnas för kvalificerade tillhandahållare och kvalificerade betrodda tjänster. Det är således en allvarlig brist i efterlevnad att erbjuda eller sälja tjänster från en verksamhet under förespegling att den är kvalificerad utan att den genomgått granskning och de processer som krävs för att en tillhandahållare eller tjänst ska vara kvalificerad. Ett sådant agerande ska kunna läggas till grund för ett beslut om sanktionsavgift.

Tillhandahållaren lämnar oriktiga eller ofullständiga uppgifter vid ansökan om att bli kvalificerad eller för att upprätthålla den statusen

För att bli en kvalificerad tillhandahållare av kvalificerade betrodda tjänster ska tillhandahållaren genomgå en bedömning av överensstämmelse. Detsamma gäller för de betrodda tjänster som tillhandahållaren vill ska vara kvalificerade.

För att upprätthålla statusen som kvalificerad ska såväl tillhandahållaren som tjänsterna omfattas av förnyade bedömningar av överensstämmelse åtminstone var 24:e månad. Vid sådana granskningar görs en omfattande genomgång av dokumentation av styrande dokument och kontroller på plats hos den som granskas. För att systemet ska fungera krävs att den sökande lämnar korrekta och sanna uppgifter vid granskningen och att de arbetar på det sättet som granskningen omfattar. Vidare ska sanningsenliga uppgifter lämnas även vid tillsyn. Dessa granskningar är en förutsättning för att en tillhandahållare av betrodda tjänster och betrodda tjänster ska bli kvalificerade. Det finns skyldigheter enligt förordningen att lita på kvalificerade betrodda tjänster och då även gränsöverskridande sådana tjänster. Tilliten till dessa tjänster bygger till stor del på den granskning som görs. Att lämna oriktiga eller ofullständiga uppgifter på detta sätt ska därmed kunna leda till ett beslut om sanktionsavgift.

Tillhandahållaren informerar inte om ändringar i verksamheten eller tillhandahållande av tjänsten

Enligt artikel 24.2 a ska tillhandahållare informera tillsynsmyndigheten om förändringar i verksamheten minst en månad i förväg, eller minst tre månader om det finns en avsikt att upphöra med verksamheten. Förändringar i verksamheten kan påverka förtroendet för tjänsten och det är därför viktigt att tillsynsmyndigheten informeras om planerade förändringar. Detta då det exempelvis kan föranleda en annan bedömning av överensstämmelse eller påverka ett tidigare beslut om status som kvalificerad. Underlåtenhet att informera tillsynsmyndigheten om förändringar i verksamheten i förtid ska därmed kunna leda till att en sanktionsavgift påförs.

Tillhandahållaren missbrukar EU-förtroendemärket för kvalificerade betrodda tjänster

Enligt artikel 23 i den ursprungliga eIDAS-förordningen får kvalificerade tillhandahållare av kvalificerade betrodda tjänster använda EU-förtroendemärket för att på ett enkelt, igenkännligt och tydligt sätt ange de kvalificerade betrodda tjänster som de tillhandahåller. Märket signalerar således att tjänsten uppfyller vissa krav som det är av stor vikt att övriga berörda aktörer kan lita på. Om EU-förtroendemärket används av tillhandahållare som inte har rätt att använda märket kan tillsynsmyndigheten besluta om sanktionsavgift.

Tillhandahållaren underlåter att rapportera säkerhetsincidenter

Kvalificerade tillhandahållare har en skyldighet enligt artikel 24.2 fb i den reviderade eIDAS-förordningen att – inom 24 timmar från händelsen – anmäla till tillsynsorganet och andra berörda, säkerhetsincidenter eller störningar av den kvalificerade betrodda tjänsten eller genomförande av åtgärder i enlighet med artikel 24.2 fa i den reviderade förordningen som har en betydande inverkan på tillhandahållandet av den betrodda tjänsten eller personuppgifter i den. Motsvarande regler finns för icke-kvalificerade tillhandahållare av betrodda tjänster i artikel 19a.1b. Incidentrapporteringen är ett viktigt verktyg för tillsynen och för att upprätthålla förtroendet för tjänsterna och tillhandahållarna. En underlåtenhet att incidentrapportera ska därmed kunna leda till en sanktionsavgift.

Tillhandahållaren följer inte ett beslut om förbud som fattats av tillsynsmyndigheten

Vid allvarliga överträdelser av eIDAS-förordningen, i både dess tidigare och reviderade form, kan tillsynsmyndigheten enligt kompletteringslagen fatta beslut om förbud för en verksamhet och att beslutet kan gälla omedelbart. Om ett sådant beslut inte följs kan tillsynsmyndigheten besluta om sanktionsavgift.

6.6.9 Förfarandet vid beslut om sanktionsavgift

Utredningens förslag: En sanktionsavgift ska endast få beslutas om den som avgiften ska tas ut av har fått tillfälle att yttra sig inom två år från det att överträdelsen ägde rum. Ett beslut om sanktionsavgift ska delges.

Sanktionsavgiften ska betalas till tillsynsmyndigheten över betrodda tjänster inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet. Sanktionsavgiften tillfaller staten.

Om sanktionsavgiften inte betalas inom rätt tid, ska tillsynsmyndigheten lämna den obetalda avgiften för indrivning. Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m. Vid indrivning får verkställighet ske enligt utsökningsbalken.

En beslutad sanktionsavgift faller bort till den del beslutet om avgiften inte har verkställts inom fem år från det att beslutet fick laga kraft.

Skälen för utredningens förslag

Ett beslut om administrativa sanktionsavgifter är som nämnts en särskilt ingripande åtgärd och det finns därför skäl att införa en bortre gräns för när en sanktionsavgift får beslutas. Den som anspråket riktar sig mot bör därför få tillfälle att yttra sig inom två år från överträdelsen. Om kommunikation enligt 25 § förvaltningslagen inte har skett inom två år från överträdelsen, med den som avgiften ska tas ut av, får en sanktionsavgift inte tas ut.

Enligt våra förslag ska underlåtenhet att incidentrapportera i vissa fall kunna medföra sanktionsavgift. En sådan överträdelse får som utgångspunkt anses ha inträffat den dag åtgärden senast skulle ha vidtagits. Huruvida en viss underlåtenhet är av sådan karaktär att den ska anses vara fortlöpande på ett sätt som inverkar på preskriptionstidpunkten, får emellertid avgöras i varje enskilt fall och ytterst av rättslämningen.

Ett beslut om sanktionsavgift är av sådan ingripande karaktär att det bör delges den betalningsskyldige enligt delgivningslagen (2010:1932).

Bestämmelser om detta bör tas in i kompletteringslagen. Bevisbördan för att kommunikation har skett ska ligga på tillsynsmyndigheten.⁸⁸

Den avgift som tillsynsmyndigheten beslutat ska kunna drivas in utan att det krävs något domstolsavgörande. Det bör därför föreskrivas att betalning av sanktionsavgift ska ske till tillsynsmyndigheten inom 30 dagar från det att beslutet om sanktionsavgift vunnit laga kraft eller annars inom den längre tid som anges i beslutet. Om betalning inte sker i tid ska myndigheten lämna den obetalda avgiften för indrivning. Verkställighet får ske enligt utsökningsbalken.

I allmänhet gäller för administrativa sanktionsavgifter att de preskriberas om verkställighet inte har skett inom fem år. Det saknas anledning att införa annan preskriptionstid än den som i allmänhet används. Preskriptionstiden bör därför vara fem år. Sanktionsavgiften bör som brukligt tillfalla staten.⁸⁹

6.6.10 Sanktionsavgift ska bygga på strikt ansvar men inte vara obligatorisk

Utredningens förslag: Regleringen av sanktionsavgift ska bygga på strikt ansvar.

Det ska inte vara obligatoriskt att ta ut sanktionsavgift för överträdelser som kan leda till sanktionsavgift.

Skälen för utredningens förslag

Systemet ska bygga på strikt ansvar

Bestämmelser om sanktionsavgift bygger som huvudregel på strikt ansvar, vilket innebär att det inte krävs uppsåt eller oaktsamhet för att ta ut sanktionsavgift. Skälen för det anges ofta vara att en sådan ordning medför en effektiv handläggning och att ifrågavarande överträdelser sällan beror på annat än uppsåt eller oaktsamhet.⁹⁰

Vi bedömer att det saknas skäl att göra avsteg från huvudregeln när det gäller överträdelser av bestämmelser för betrodda tjänster. Vi föreslår därför en ordning som bygger på strikt ansvar, utan krav på

⁸⁸ Jfr prop. 2017/18:205 s. 74.

⁸⁹ Jfr prop. 2020/21:186 s. 41 f.

⁹⁰ Jfr exempelvis prop. 2017/18:232 s. 324 och prop. 2020/21:186 s. 36.

uppsåt eller oaktsamhet. För att en sanktionsavgift ska kunna tas ut ska det alltså vara tillräckligt att en överträdelse har ägt rum.

Eftersom det inte finns något formellt krav på uppsåt eller oaktsamhet saknas det skäl att föra in en upplysning om att avgiftsskyldigheten bygger på strikt ansvar i kompletteringslagen.⁹¹

Det ska inte vara obligatoriskt att ta ut sanktionsavgift

Eftersom bestämmelser om sanktionsavgifter ska vara likabehandlande, objektiva och proportionerliga är det ofta motiverat att begränsa utrymmet för skönsmässiga bedömningar av när sanktionsavgift ska utgå eller inte. Bestämmelser om sanktionsavgifter är därför vanligen obligatoriska när förutsättningar för en sådan ordning finns.

Enligt lagen om informationssäkerhet för samhällsviktiga och digitala tjänster gäller exempelvis att sanktionsavgifter *ska* tas ut vid överträdelser, om det inte finns förutsättningar att efterge avgiften. Enligt regeringen var behovet av att säkerställa likabehandling särskilt starkt för sanktionsavgifter enligt den lagen, eftersom utgångspunkten var att flera tillsynsmyndigheter skulle tillämpa bestämmelserna.⁹² Även för överträdelser av regelverket om cybersäkerhetscertifiering gäller enligt lag (2021:553) med kompletterande bestämmelser till EU:s cybersäkerhetsakt att den nationella myndigheten för cybersäkerhetscertifiering *ska* besluta att ta ut sanktionsavgift. Regeringen angav som skäl för bedömningen att tillsynsmyndighetens möjligheter till mer skönsmässiga bedömningar som utgångspunkt bör vara begränsade med hänsyn till behovet av likabehandling, objektivitet och proportionalitet. Vidare anfördes att, trots det komplexa regelverket, övervägande skäl talade för att det skulle vara obligatoriskt att döma ut sanktionsavgift. Enligt regeringen skulle det minska utrymmet för skönsmässiga bedömningar och framstod som mest ändamålsenligt vid mer allvarliga överträdelser av regelverket.⁹³

Enligt brottsdatalagen (2018:1177) gäller i stället att sanktionsavgift *får* tas ut vid vissa överträdelser. Det motiverades med att reglerna om personuppgiftsbehandling är mycket komplexa och att det skulle ställa alltför höga krav på de personuppgiftsansvariga samt lägga en orimlig börda på tillsynsmyndigheten om varje överträdelse

⁹¹ Jfr prop. 2020/21:194 s. 99.

⁹² Se prop. 2017/18:205 s. 69 f.

⁹³ Se prop. 2020/21:186 s. 37.

skulle leda till sanktionsavgift.⁹⁴ Motsvarande gäller enligt säkerhetsskyddslagen (2018:585). I förarbetena till lagen angavs som skäl att säkerhetsskyddslagstiftningen innehåller krav på komplexa bedömningar, exempelvis om vilka skyddsvärden som finns i en verksamhet. Vidare att det i undantagsfall kan vara svårt att bedöma om en aktör faktiskt bedriver säkerhetskänslig verksamhet, dvs. är en verksamhetsutövare som omfattas av säkerhetsskyddslagens krav. Enligt regeringen kunde det vid bedömningen av kraven i vissa fall finnas behov av att aktören tar kontakt med tillsynsmyndigheten och informerar om sin verksamhet. En reglering med obligatoriska sanktionsavgifter bedömdes inte främja ett sådant utbyte. Därutöver angavs att flera tillsynsmyndigheter ska tillämpa bestämmelserna som skäl för att det inte skulle vara obligatoriskt.⁹⁵

Som redovisats inledningsvis (se avsnitt 6.6.7) ansåg regeringen vid införandet av kompletteringslagen att kraven på tillhandahållare av betrodda tjänster innefattar bedömningsmoment och lämplighetsöverväganden som medför att överträdelse av förordningens bestämmelser ofta kan vara svåra att konstatera och kan kräva omfattande utredning. Vi delar den bedömningen och kan konstatera att den reviderade förordningen inte medför någon annan slutsats i angivet avseende.

Kretsen av aktörer som tillhandahåller betrodda tjänster är skiftande och omfattar såväl stora som små företag, liksom offentliga aktörer och potentiellt även privatpersoner. Vid samtal med företrädare för PTS har framkommit att myndigheten inte sällan har kontakt med olika aktörer vilket, på samma sätt som för tillsynsmyndigheten enligt säkerhetsskyddslagen, anges främja ett värdefullt utbyte. Ett sådant utbyte kan antas bli särskilt värdefullt med hänsyn till att gränsdragningsfrågor i förhållande till regelverket enligt NIS2-direktivet kommer att behöva göras.

Det är inte alldeles tydligt hur olika faktorer i tidigare lagstiftningsärenden har påverkat bedömningen av när det ska vara obligatorisk att besluta om sanktionsavgifter eller inte. Att flera tillsynsmyndigheter ska tillämpa bestämmelserna har exempelvis anförts som skäl både för och emot en sådan ordning.

Enligt vår bedömning talar emellertid i fråga om sanktioner för betrodda tjänster såväl den komplexa materian som att det är av stor

⁹⁴ Se prop. 2017/18:232 s. 324 f.

⁹⁵ Se prop. 2020/21:194 s. 99 ff.

vikt att främja ett utbyte mellan tillsynsmyndigheten och berörda aktörer med styrka för att tillsynsmyndigheten ska kunna avgöra om en sanktionsavgift ska beslutas eller inte. Mot angiven bakgrund föreslår vi en ordning där det inte ska vara obligatoriskt för tillsynsmyndigheten att besluta om sanktionsavgift.

6.6.11 Sanktionsavgiftens storlek

Utredningens förslag: Sanktionsavgiften för fysiska personer ska bestämmas till lägst 5 000 kronor och högst ett belopp motsvarande 5 miljoner euro.

Sanktionsavgiften för juridiska personer ska bestämmas till lägst 5 000 kronor och högst det högsta av ett belopp motsvarande 5 miljoner euro respektive en procent av den totala globala årsomsättningen för det företag som tillhandahållaren av betrodda tjänster tillhörde under det räkenskapsår som föregick det år då överträdelsen inträffade.

När sanktionsavgiftens storlek bestäms ska särskild hänsyn tas till berörd enhets storlek, affärsmodeller och överträdelsernas allvar.

Sanktionsavgiften ska få sättas ned helt eller delvis om överträdelsen är ringa eller ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften.

Skälen för utredningens förslag

Enligt artikel 16.2 i den reviderade eIDAS-förordningen ska medlemsstaterna säkerställa att överträdelser av förordningen medför maximala administrativa sanktionsavgifter som uppgår till minst fem miljoner euro om tillhandahållaren är en fysisk person eller, om tillhandahållaren är en juridisk person, det högsta av fem miljoner euro respektive en procent av den totala globala årsomsättningen för det företag som tillhandahållaren av betrodda tjänster tillhörde under det räkenskapsår som föregick det år då överträdelsen inträffade. Några ytterligare bestämmelser om hur sanktionsavgifterna ska vara utformade innehåller förordningen inte.

Sanktionsavgifter ska vara effektiva, proportionerliga och avskräckande. Bestämmelserna om betrodda tjänster omfattar såväl enskilda

som myndigheter och företag. Aktörerna kommer alltså att skilja sig mycket från varandra vad gäller t.ex. storlek och ekonomiska förutsättningar. Därmed kommer också det belopp som framstår som avskräckande skilja sig åt väsentligt mellan de olika aktörerna. Detta är omständigheter som enligt vår bedömning motiverar ett vidsträckt beloppintervall.

Den reviderade förordningen anger som framgått inte något minimibelopp för sanktionsavgifternas storlek. Utredningen om genomförande av NIS2- och CER-direktiven lämnade i sitt delbetänkande förslaget att lägstanivån för sanktionsavgift enligt det regelverket även fortsättningsvis ska vara 5 000 kronor. Utredningen anförde att den inte funnit skäl att höja beloppet som överensstämmer med lägsta belopp för företagsbot.⁹⁶

Regelverket för betrodda tjänster är delvis överlappande med det som gäller enligt NIS2-direktivet. En och samma aktör kommer därför i vissa fall, vid ett otillåtet agerande, att överträda båda regelverken samtidigt. Det finns således anledning att eftersträva viss överensstämmelse för att undvika oförutsägbarhet eller en ordning där skillnaderna leder till anpassningar till följd av storleken på förväntad sanktionsavgift. Därtill kommer att den angivna lägsta maximala sanktionsavgiften enligt NIS2-direktivet är högre än den för eIDAS-förordningen vilket motiverar bedömningen att lägsta sanktionsbelopp enligt eIDAS-förordningen inte bör vara högre satt än vad som gäller enligt NIS2-direktivet. Inte heller ett lägre belopp bör komma i fråga. Lägstanivån för sanktionsavgift bör således vara 5 000 kronor för såväl fysiska som juridiska personer.

Såvitt avser det högsta beloppet anges i den reviderade förordningen som framgått att beloppet, beroende på vilket som är högst, antingen ska uppgå till ett fast belopp eller beräknas utifrån årsomsättningen. Som lägst ska det högsta fasta beloppet uppgå till fem miljoner euro.

I förarbetena till lagen med kompletterande bestämmelser till EU:s cybersäkerhetsakt anförde regeringen att en maximal avgift om högst tio miljoner kronor bedömts utgöra en effektiv, proportionell och avskräckande sanktion vid allvarliga överträdelser av bl.a. lagen om informationssäkerhet för samhällsviktiga och digitala tjänster. Mot den bakgrunden och med beaktande av förekomsten av stora globala aktörer på IKT-marknaden, ansåg regeringen att det högsta beloppet

⁹⁶ Se *Nya regler om cybersäkerhet* (SOU 2024:18), s. 288 f.

för en sanktionsavgift enligt den föreslagna lagen skulle bestämmas till 15 miljoner kronor.⁹⁷

Vid en jämförelse med andra nationella sanktionsbestämmelser står det klart att redan det, i den reviderade eIDAS-förordningen föreskrivna, lägsta maximala beloppet väl överstiger vad som enligt andra regelverk har bedömts utgöra avskräckande nivåer. I ljuset därav har vi inte kunnat identifiera några tungt vägande skäl för att sanktionsavgiften ska sättas högre än det som minst krävs enligt den reviderade förordningen för att verka avskräckande. För stora aktörer med betydande omsättning finns det dessutom, med hänsyn till det rörliga alternativet, utrymme för att bestämma ett högre belopp. Vi föreslår därför att det högsta fasta beloppet ska kunna bestämmas till ett belopp motsvarande fem miljoner euro. Beloppet är enligt förordningen inte knutet till växelkursen en viss dag. Vilket belopp som motsvarar en miljon euro bör därför bestämmas utifrån kronkursen den dag då beslut om sanktionsavgift meddelas.⁹⁸

Vid bestämmande av sanktionsavgiften i det enskilda fallet bör hänsyn tas till samtliga relevanta omständigheter. I den reviderade förordningen lyfts fram att vederbörlig hänsyn ska tas till berörda enheters storlek, affärsmodeller och överträdelsernas allvar vid bestämmande av sanktionsavgiften.⁹⁹ I vilken omfattning angivna parametrar ska beaktas eller vilka närmare omständigheter dessa ska anses rymma redovisas inte. Som nämnts omfattas inte heller bestämmelserna om sanktioner av kommande genomförandeakter.

Regeringen ansåg vid tillkomsten av lagen om informations säkerhet för samhällsviktiga och digitala tjänster att det – vid bestämmande av sanktionsavgiften – var särskilt viktigt att beakta den skada eller risk för skada som uppstått till följd av överträdelserna, om aktören tidigare begått en överträdelse och de kostnader som aktören undvikit till följd av regelöverträdelserna.¹⁰⁰ Vi menar att dessa omständigheter gör sig gällande även för överträdelser av regelverket för betrodda tjänster och att samtliga dessa ryms inom ramen för bedömningsgrunden *överträdelsernas allvar*. Någon reglering enligt vilken hänsyn ska tas till berörd enhets affärsmodell har vi inte funnit men enligt vår bedömning bör det exempelvis kunna beaktas i förmildrande rikt-

⁹⁷ Se prop. 2020/21:186 s. 38.

⁹⁸ Jfr prop. 2016/17:173 s. 556.

⁹⁹ Skälpunkt 44 i den reviderade eIDAS-förordningens ingress.

¹⁰⁰ Se prop. 2017/18:205 s. 71.

ning om det har varit fråga om en ideell aktör som gjort sig skyldig till överträdelsen.

Eftersom avgiftsskyldigheten bygger på strikt ansvar bör det vara möjligt för tillsynsmyndigheten att jämka eller helt sätta ned sanktionsavgiften om överträdelsen är ringa eller ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften. Det kan exempelvis gälla om en verksamhetsutövare drabbats av sanktionsavgift enligt något annat regelverk för i princip samma brott. En bestämmelse som ger tillsynsmyndigheten utrymme att jämka eller helt sätta ner avgiften bör därför tas in i kompletteringslagen. Möjligheten att sätta ner avgiften bör tillämpas restriktivt och endast när det skulle te sig oskäligt att ta ut avgiften.¹⁰¹

6.6.12 Hinder mot sanktionsavgift

Utredningens förslag: Tillsynsmyndigheten över betrodda tjänster får inte besluta om sanktionsavgift om överträdelsen omfattas av ett föreläggande om vite och överträdelsen ligger till grund för en ansökan om utdömmande av vitet.

Skälen för utredningens förslag

I det sjunde tilläggsprotokollet till Europakonventionen och i EU:s rättighetsstadga finns bestämmelser om rätten att inte bli lagförd eller straffad två gånger för samma brott (gärning), det s.k. dubbelprövningsförbudet.

Begreppet straff i den mening som avses i Europakonventionen har i flertalet tidigare lagstiftningsärenden ansetts omfatta vite. Om ett vite har dömts ut bör det därför inte vara möjligt att besluta om en sanktion – administrativ eller straffrättslig – för samma sak. Den avgörande tidpunkten för när sådant hinder uppkommer bör anses vara när det inleds en domstolsprocess angående frågan om utdömmande av vite. När tillsynsmyndigheten har ansökt om utdömmande av vitet bör alltså tillsynsmyndigheten vara förhindrad att besluta om sank-

¹⁰¹ Jfr prop. 2017/18:205 s. 72.

tionsavgift för en överträdelse som omfattas av vitesföreläggandet.¹⁰² En bestämmelse om detta bör tas in i kompletteringslagen.

6.7 Överklagande

Utredningens förslag: Bestämmelsen om överklagande i lagen med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering ska ändras. Av bestämmelsen ska framgå att den omfattar även de tillkommande beslut som enligt våra förslag får fattas enligt EU:s reviderade förordning om elektronisk identifiering och rättsakter som har meddelats med stöd av förordningen, samt enligt svenska författningar i anslutning till EU-förordningen.

Skälen för utredningens förslag

En bestämmelse om rätt att överklaga tillsynsmyndighetens beslut enligt EU:s förordning om elektronisk identifiering och rättsakter som har meddelats med stöd av förordningen, samt enligt kompletteringslagen och föreskrifter som har meddelats med stöd av densamma finns redan i 8 § kompletteringslagen.

Våra förslag innebär att ytterligare beslut som påverkar enskilda kommer att fattas av utpekade myndigheter. Dessa beslut ska vara möjliga att överklaga. Besluten ska på samma sätt som tidigare få överklagas till allmän förvaltningsdomstol. I likhet med vad som är huvudregeln för överklagande av förvaltningsbeslut bör prövningstillstånd krävas vid överklagande till kammarrätten.

¹⁰² Se prop. 2020/21:186 s. 41 och där gjorda hänvisningar.

6.8 Identitetsplånverkens användningsområden för nationell effektivitet och nytta

Utredningens bedömning: En närmare analys av hur den europeiska digitala identitetsplånverket ska kunna användas ändamålsenligt och för största möjliga nationella effektivitet och nytta bör genomföras när innehållet i kommande genomförandeakter och resultaten av de storskaliga pilotprojekten är kända.

Skälen för utredningens bedömning

I vårt uppdrag ingår att utreda hur en europeisk digital identitetsplånverk kan användas ändamålsenligt för största möjliga nationella effektivitet och nytta.

Den reviderade eIDAS-förordningen trädde i kraft den 20 maj 2024 och det pågår i skrivande stund ett omfattande arbete med att testa såväl identitetsplånverket som användningsfall för densamma i de storskaliga pilotprojekt som kommissionen har utlyst. Vidare har det stora antalet genomförandeakter som närmare kommer att precisera funktioner och förfaranden ännu inte antagits. Mot angiven bakgrund är det enligt vår bedömning i nuläget inte möjligt att på ett konkret sätt beskriva hur den europeiska digitala identitetsplånverket ska användas för största möjliga nationella effektivitet och nytta. Genom att ta del av målsättningen för de storskaliga pilotprojekten går det dock att få en bild över hur den europeiska digitala identitetsplånverket är avsedd att bidra till nationell effektivitet och nytta.

Pilotprojekten, som också beskrivs i avsnitt 4.7.3, testar identitetsplånverket noggrant i en rad vardagliga scenarier. Avsikten är att undersöka hur identitetsplånverket kan tillhandahålla lösningar inom följande områden:

- Åtkomst till myndighetstjänster: Säker åtkomst till digitala offentliga tjänster, t.ex. att ansöka om pass eller körkort, lämna in skatter eller få tillgång till socialförsäkringsinformation.
- Öppna bankkonto: verifiering av en identitet när ett bankkonto öppnas online.

- SIM-registrering: identitetsbevis för för- och efterbetalda SIM-kortsavtal vilket ska minska bedrägerier och kostnader för mobilnätoperatörer.
- Mobilt körkort: Lagring och presentation av ett mobilt körkort online och vid fysisk interaktion, t.ex. om en förare stoppas vid sidan av vägen.
- Undertecknande av kontrakt: Skapa säkra elektroniska underskrifter för undertecknande av avtal online för att eliminera behovet av pappersdokument och fysiska underskrifter.
- Anspråk på recept: Tillhandahållande av uppgifter om recept till apotek och initiering av expediering av läkemedel.
- Resor: Presentera information från resehandlingar (t.ex. pass, visum), vilket möjliggör snabb och enkel åtkomst när en användare går igenom flygplatsens säkerhets- och tullkontroll.
- Organisatoriska digitala identiteter: Bevis om att en användare är en legitim företrädare för en organisation.
- Betalningar: Verifiering av en användares identitet när en betalning görs online.
- Certifiering av utbildning: Bevis på innehav av utbildningsmeriter, såsom examensbevis, examina och certifikat som gör det lättare att söka jobb eller vidareutbildning.
- Tillgång till socialförsäkringsförmåner: En europeisk digital identitetsplånbok kan användas för att på ett säkert sätt få tillgång till en användares socialförsäkringsuppgifter och socialförsäkringsförmåner (t.ex. pensions- och invaliditetsförmåner). Den kan också användas för att underlätta den fria rörligheten genom att lagra handlingar som det europeiska sjukförsäkringskortet.¹⁰³

På ett generellt plan står det alltså klart att avsikten är att den europeiska digitala identitetsplånboken ska bidra till betydande effektivitetsvinster för såväl individer som offentliga och privata aktörer.

Möjligheten att kunna samla relevanta uppgifter och intyg på ett och samma ställe kan givetvis förväntas underlätta enskildas vardag

¹⁰³ <https://digital-strategy.ec.europa.eu/sv/policies/eudi-wallet-implementation> (hämtad 2024-05-19).

och yrkesliv samt bidra till en ökad digitalisering i samhället. Vilka personuppgifter som delas ska som framgått vara helt upp till användaren som kan välja att, i stället för att visa upp en fysisk id-handling som innehåller flertalet uppgifter, exempelvis endast dela sitt födelseår om ytterligare uppgifter inte krävs. Vidare ska det vara möjligt att dela uppgifter helt anonymt. Således kommer identitetsplånboken erbjuda ett högt skydd för den personliga integriteten och förhindra oönskad profilering.

Identitetsplånboken kan vidare förväntas bidra till ökad effektivisering inom olika offentliga sektorer. I den reviderade eIDAS-förordningens ingress (skäl 19) framhålls att europeiska digitala identitetsplånböcker kan användas för att tillgodose de institutionella behoven vid offentliga förvaltningar. Där anges vidare att det i många sektorer är viktigt med autentisering offline, bland annat i hälso- och sjukvårdssektorn, där tjänsterna ofta tillhandahålls vid direkta kontakter, och att e-recept bör kunna autentiseras med hjälp av QR-koder eller liknande tekniker.

I samband med utredningens expertgruppsmöten har identitetsplånbookens funktioner framhållits när det finns behov av att administrera komplexa behörigheter inom olika sektorer. Ett exempel är forskningssektorn vars strukturer kan vara organisatoriskt och tekniskt komplexa eftersom olika krav på kompetenser och åtkomst kan krävas för olika projekt och individer. Exempelvis kan en forskare vara behörig att ta del av patientdata i ett visst projekt, men ha en helt annan behörighet i ett annat. Att via identitetsplånboken kunna koppla behörighet och åtkomst till vissa roller kan således förväntas innebära stora effektivitetsvinster. Motsvarande behov kan antas föreligga inom exempelvis sjukvården eller rättsväsendet.

Inom exempelvis högskolesektorn kan identitetsplånboken användas av studenter och forskare för att lagra och visa upp studiemeriter. Meriterna kan via identitetsplånboken – om användaren önskar – på ett enklare sätt jämföras och matchas mot kompetenser som offentlig sektor och privata aktörer efterfrågar.

För offentlig sektor, men också för privata aktörer, kan anställningsprocesser effektiviseras, särskilt i de fall krav på viss yrkeslegitimation föreligger. Genom att använda identitetsplånboken kan vårdpersonal styrka sin behörighet via hämtade attributsintyg. Även för privata aktörer kan identitetsplånböckerna medföra effektivitets-

vinster exempelvis genom nya möjligheter att på ett enhetligt sätt identifiera sig och sina kunder inom hela EU.

Sammanfattningsvis står det klart att den europeiska digitala identitetsplån-boken kommer att ha ett vidsträckt tillämpningsområde. Arbetet med att utvärdera hur den europeiska digitala identitetsplån-boken kan användas för största möjliga nationella nytta bör – i avvaktan på resultaten från de storskaliga pilotprojekten – ske fortlöpande, förslagsvis i samråd med de myndigheter som för Sveriges räkning deltar i de storskaliga pilotprojekten. En närmare analys av hur den europeiska digitala identitetsplån-boken ska kunna användas ändamålsenligt och för största möjliga nationella effektivitet och nytta kan enligt vår bedömning emellertid genomföras först när innehållet i kommande genomförandeakter och resultaten av de storskaliga pilotprojekten är kända.

6.9 Missbruk eller annan otillåten användning av identitetsplån-boken

Utredningens bedömning: De fördelar som EU:s reviderade förordning om elektronisk identifiering erbjuder för skydd av den personliga integriteten kan samtidigt medföra risker för individen och samhället till följd av sämre förutsättningar för brottsförebyggande och brottsutredande arbete kopplat till informationsinhämtning om elektroniska transaktioner.

Frågan om hur den identitetsrelaterade brottsligheten kopplat till europeiska digitala identitetsplån-böcker ska hanteras måste fortsättningsvis vara högt prioriterad.

Skälen för utredningens bedömning

Fokus på användarnas integritet

I vårt delbetänkande redogjorde vi för den identitetsrelaterade brottsligheten som begås bl.a. med användning av digitala identiteter.¹⁰⁴ På samma sätt som för den statliga e-legitimationen bedömer vi att brotts-

¹⁰⁴ *En säker och tillgänglig digital identitet* (SOU 2023:61), s. 109 ff.

lighet kopplad till användningen av den europeiska digitala identitetsplånboken behöver hanteras.

I den reviderade eIDAS-förordningen står, även om det är tydligt att också övriga säkerhetsaspekter är av avgörande betydelse, den enskilda användarens säkerhet kopplad till den personliga integriteten i fokus. I förordningens ingress (skäl 13) anges till att börja med att de europeiska digitala identitetsplånböckerna bör ha en funktion i form av en gemensam instrumentpanel som möjliggör för användarna att ha en högre grad av öppenhet, integritet och kontroll av sina data. Instrumentpanelen ska innehålla en översikt över alla förlitande parter med vilka användaren delar data, inklusive attribut, och vilken typ av uppgifter som delats med varje förlitande part. Användarna bör enligt vad som föreskrivs ges möjlighet att spåra alla transaktioner som utförs genom den europeiska digitala identitetsplånboken med åtminstone följande uppgifter: tidpunkt och datum för transaktionen, identifiering av motparten, begärda personuppgifter och delade uppgifter. Genom instrumentpanelen ska användaren kunna begära att en förlitande part omedelbart raderar personuppgifter och enkelt kunna rapportera den förlitande parten till den behöriga nationella data-skyddsmyndigheten.

Enligt artikel 5a.14 ska användarna ha full kontroll över användningen av, och uppgifterna i, sin europeiska digitala identitetsplånbok. Tillhandahållaren av identitetsplånboken får inte samla in information om användningen av identitetsplånboken som inte är nödvändig för tillhandahållandet av tjänster relaterade till densamma. Tillhandahållaren får inte heller kombinera personidentifieringsuppgifter eller några andra personuppgifter som lagras, eller som rör användningen av den europeiska digitala identitetsplånboken med personuppgifter från andra tjänster eller från tredjepartstjänster och som inte krävs för tillhandahållandet av tjänster relaterade till den europeiska digitala identitetsplånboken, om inte användaren uttryckligen har begärt detta.

Vidare ska det tekniska ramverket för den europeiska digitala identitetsplånboken, enligt artikel 5a.16 a, inte tillåta tillhandahållare av elektroniska attributsintyg *eller någon annan part* att – efter utfärdandet av attributsintyget – erhålla data som gör det möjligt att spåra, länka, korrelera transaktioner eller användarbeteende eller på annat sätt få kännedom om transaktioner eller användarbeteende, såvida inte användaren uttryckligen har gett sitt tillstånd. I förordningens ingress (skäl 32) framhålls att tillhandahållare av europeiska digitala

identitetsplånböcker bör säkerställa icke-observerbarhet genom att inte samla in uppgifter och inte ha insyn i de transaktioner som utförs av användarna av den europeiska digitala identitetsplånboken. Sådan icke-observerbarhet anges innebära att tillhandahållarna inte kan se detaljerade uppgifter om användarens transaktioner. I specifika fall, baserat på användarnas tidigare uttryckliga samtycke för vart och ett av dessa specifika fall, skulle tillhandahållare av europeiska digitala identitetsplånböcker kunna beviljas tillgång till den information som krävs för tillhandahållandet av en viss tjänst som gäller europeiska digitala identitetsplånböcker.

Bestämmelser om säkerhet kopplat till annat än integritetskydd

I förordningen finns också bestämmelser som behandlar säkerhetsaspekter kopplat till annat än användarens personliga integritet. Av artikel 5a.12 framgår exempelvis att de europeiska digitala identitetsplånböckerna ska säkerställa inbyggd säkerhet. I förordningens ingress (skäl 31) förtydligas att de europeiska digitala identitetsplånböckerna bör ha inbyggd säkerhet och innefatta avancerade säkerhetsfunktioner för att skydda mot identitetsstöld och annan datastöld, tillgänglighetsförlust och alla andra cyberhot. Säkerheten bör enligt vad som anges innefatta toppmoderna krypterings- och lagringsmetoder som är tillgängliga och dekrypterbara endast för användaren, och som förlitar sig på totalsträckskrypterad kommunikation med andra europeiska digitala identitetsplånböcker och förlitande parter. Dessutom bör de europeiska digitala identitetsplånböckerna kräva en säker, uttrycklig och aktiv bekräftelse av användaren för de operationer som utförs via de europeiska digitala identitetsplånböckerna.

Medlemsstaterna kommer vidare att behöva säkerställa att alla identitetsplånböcker som tillhandahålls är certifierade, inbegripet att certifieringen är giltig i högst fem år och villkoras av att en sårbarhetsbedömning genomförs med intervall om två år enligt artikel 5c.1, 2 och 3 (se avsnitt 6.3.7). Vidare kommer tillsynsmyndigheter att utöva tillsyn över såväl tillhandahållare av europeiska digitala identitetsplånböcker etablerade i medlemsstaten och – genom förebyggande och uppföljande kontroller – säkerställa att såväl tillhandahållare av som de utfärdade identitetsplånböckerna uppfyller kraven i förordningen (se avsnitt 6.6.1). Således omgärdas identitetsplånböckerna

av funktioner och institut som är avsedda att säkerställa en hög säkerhet för systemet i dess helhet.

En ytterligare säkerhetsaspekt är att den europeiska identitetsplån-boken ska utfärdas på tillitsnivå hög. Tillitsnivån på e-legitimationen avgör hur tillförlitligt det är att personen som identifierar sig är den man utger sig för att vara. I dag är de e-legitimationer som används i Sverige på tillitsnivå väsentlig, dvs. en nivå under tillitsnivå hög.

I förordningens ingress (skäl 18) anges att det är av stor betydelse för att säkerställa förtroende för och en bred spridning av europeiska digitala identitetsplånböcker att unionsmedborgare och invånare i unionen skyddas mot obehörig eller bedräglig användning av europeiska digitala identitetsplånböcker. Vidare framhålls (skäl 35) att medlemsstaterna i samarbete med den privata sektorn, forskare och den akademiska världen, bör utveckla utbildningsprogram som syftar till att stärka de digitala färdigheterna hos sina medborgare och invånare, särskilt för utsatta grupper, såsom personer med funktionsnedsättning och äldre personer. Medlemsstaterna bör enligt vad som anges öka medvetenheten om fördelarna och riskerna med europeiska digitala identitetsplånböcker genom informationskampanjer.

*Befintliga möjligheter att motverka
och utreda brott kommer att förändras*

Förordningens krav på att det inte ska vara möjligt för någon annan än användaren att på olika sätt hantera data kopplad till en viss identitetsplånbok är tydliga. Det är också tydligt att identitetsplånbokens tekniska utformning ska vara säker. En säker utformning kan emellertid inte ensamt förhindra de brott som begås med användning av e-legitimationer, och därmed inte heller de som kommer att begås med användning av identitetsplånboken. Den identitetsrelaterade brottsligheten begås, som vi redovisade i vårt delbetänkande, i stor utsträckning antingen genom att användaren utnyttjas på olika sätt eller genom användande av falska identiteter.¹⁰⁵ Om det ska vara möjligt att förebygga och motverka, men framför allt utreda brott som inbegriper olika former av digitala transaktioner, är det därför av stor betydelse att det går att ta del av data kopplade till ifrågavarande transaktioner.

¹⁰⁵ En säker och tillgänglig digital identitet (SOU 2023:61), s. 109 ff.

Befintliga utfärdare av e-legitimationer, exempelvis Finansiell ID-Teknik BID AB som äger och förvaltar BankID, arbetar kontinuerligt och aktivt med säkerhetsarbete och utveckling i syfte att öka säkerheten vid utgivning och användning av e-legitimationer.¹⁰⁶ I en artikel i Svensk Juristtidning från 2023 framhålls från Finansiell ID-Teknik BID AB:s sida två grundläggande förutsättningar för att stoppa den negativa spiralen av obehörig användning av e-legitimationer. Dessa anges vara dels lagstiftning som avgör hur och när brottsutredande- och andra myndigheter, samt olika finansiella verksamhetsutövare kan och får samarbeta och utbyta information med varandra, dels strängare identifieringskrav vid inskrivning i folkbokföringen. Vidare framhålls betydelsen av hur förlitande parter utformar sina e-tjänster för bedragares möjligheter att lura en användare. Enligt vad som anges i artikeln avses t.ex. att förlitande parter kan kräva olika förstärkningsfunktioner samt tydlig underskrifts- och avsiktstext vid identifiering i sin tjänst. Slutligen framförs att det kan finnas skäl för en förlitande part att spara identifieringsintyg respektive elektronisk underskrift eftersom de kan utgöra bevisning vid en eventuell tvist.¹⁰⁷

Samtliga föreslagna åtgärder framstår som ändamålsenliga och viktiga. Vi kan dock konstatera att eIDAS-regelverket – i synnerhet till följd av bestämmelsen i artikel 5a.16 a – synes begränsa dels möjligheten till informationsutbyte mellan myndigheter, dels möjligheten för förlitande parter att spara identitetsintyg och elektroniska underskrifter såvida inte användaren har godkänt det. Övriga föreslagna åtgärder kan således bli än mer betydelsefulla att genomföra.

Brottsutredande myndigheter kan i dagsläget ha stor nytta av data som utvisar hur och när en e-legitimation har använts. Vid utredningens kontakter med företrädare för Ekobrottsmyndigheten har det framkommit att sådana data i vissa fall är av helt avgörande betydelse för möjligheten att utreda företrädesvis ekonomisk, men också annan brottslighet. Enligt uppgift från Finansiell ID-Teknik BID AB genererade bankerna knappt 44 000 myndighetsrapporter under 2023, av vilka merparten var till Polismyndigheten.

Vi bedömer att redovisade bestämmelser om lagrings-, delnings- och uppgiftsminimering i den reviderade förordningen i princip omöjliggör för brottsutredande myndigheter att – när en europeisk

¹⁰⁶ Se t.ex. www.bankid.com/om-oss/nyheter/okad-sakerhet-nar-du-skaffar-nytt-mobilt-bankid (hämtad 2024-06-03).

¹⁰⁷ SvJT 2023 s. 442.

digital identitetsplånbok har använts – få tillgång till uppgifter som i nuläget kan utgöra en förutsättning för att utreda brott. Förutsättningarna för att inhämta data kopplat till användningen av en europeisk digital identitetsplånbok kan i stället jämföras med när en fysisk legitimationshandling använts som brottsverktyg, vilket i normalfallet inte heller efterlämnar spår. Skillnaden mellan de två är dock att brott som begås digitalt kan ske snabbare och i större skala.

Det förebyggande arbete som befintliga e-legitimationsutfärdare genomför och som syftar till att upptäcka avvikande aktivitet i samband med användande av e-legitimationen kommer sannolikt inte heller att kunna genomföras vid användning av den europeiska digitala identitetsplånboken.

Sammanfattningsvis kan det konstateras att brott som begås med användning av identitetsplånböcker kommer att behöva förebyggas och utredas på andra sätt än via transaktionsdata. Vi har av tidsmässiga skäl och på grund av att relevanta genomförandeakter ännu inte antagits inte kunnat genomföra någon mer fullständig genomlysning av vilka konkreta problem kopplade till missbruk av identitetsplånboken som kan komma att uppstå. I sammanhanget kan dock nämnas att Svenska Bankföreningen redan 2021 framförde synpunkter och farhågor i ett yttrande till Infrastrukturdepartementet. Bland dessa fanns, utöver risken för att transaktionsbaserad riskinformation kommer att saknas, exempelvis att en person med medborgarskap i olika länder kan få identitetsplånböcker utfärdade i fler än ett land, vilket enligt bankföreningen inte är i linje med intentionerna i penningtvättslagstiftningen.¹⁰⁸ Vid utredningens kontakter med företrädare för Svenska Bankföreningen har framkommit att farhågorna kvarstår.

Vi bedömer sammanfattningsvis att frågan om hur den identitetsrelaterade brottsligheten kopplat till europeiska digitala identitetsplånböcker ska hanteras fortsättningsvis måste vara högt prioriterad. De åtgärder som förordningen tillåter i form av informationskampanjer eller andra förstärkningsfunktioner i samband med användandet, liksom begränsningar i antalet fysiska id-handlingar och stränga identifieringskrav i folkbokföringen, bör ges stor plats i ett framtida säkerhetsarbete för att skapa så goda förutsättningar som möjligt för enskilda att upptäcka om de utsätts för ett brottsligt agerande.

¹⁰⁸ Bankföreningens synpunkter på EU-kommissionens förslag till förordning om ändring av EU:s förordning om elektronisk identifiering i fråga om fastställande av en ram för en europeisk digital identitet (ändring av förordning 910/2014), (ref nr: i2021/01737), 2021-11-19.

7 Ikraftträdande- och övergångsbestämmelser

Utredningens förslag: Lämnade författningsförslag ska träda i kraft den 1 oktober 2025. Nuvarande bestämmelser ska fortfarande gälla för överträdelser som har ägt rum före ikraftträdandet.

Skälen för utredningens förslag

Som redan redovisats publicerades den reviderade eIDAS-förordningen i Europeiska unionens officiella tidning den 30 april 2024 och trädde därmed i kraft den 20 maj i år (se artikel 52).

Förordningen är direkt tillämplig i Sverige och övriga medlemsstater. Några särskilda åtgärder för att den ska börja gälla behövs därför inte. I förordningen finns även reviderade övergångsbestämmelser i artikel 51. Dessa föreskriver, i likhet med tidigare övergångsbestämmelser, att säkra anordningar för skapande av underskrifter, vilkas överensstämmelse har fastställts i enlighet med artikel 3.4 i det upphävda signaturdirektivet¹, ska anses som kvalificerade anordningar för skapande av elektroniska underskrifter enligt den reviderade eIDAS-förordningen, dock endast till och med den 21 maj 2027 (artikel 51.1). Likaså anges att kvalificerade certifikat som har utfärdats för fysiska personer enligt nämnda direktiv ska anses som kvalificerade certifikat för elektroniska underskrifter enligt den reviderade eIDAS-förordningen. Även för sådana certifikat införs nu en tidsbegränsning, men i dessa fall till den 21 maj 2026 (artikel 51.2).

Slutligen finns också bestämmelser som gäller för vissa kvalificerade tillhandahållare av betrodda tjänster. För det första får, under angivna

¹ Europaparlamentets och rådets direktiv 1999/93/EG av den 13 december 1999 om ett gemenskapsramverk för elektroniska signaturer. Direktivet upphävdes den 1 juli 2016, samtidigt som eIDAS-förordningen började tillämpas.

förutsättningar, förvaltning av kvalificerade anordningar för skapande av elektroniska underskrifter och stämplat på distans utföras utan att status som kvalificerad för tillhandahållandet av dessa förvaltnings-tjänster behöver erhållas förrän den 21 maj 2026 (artikel 51.3). För det andra har sådana kvalificerade tillhandahållare av betrodda tjänster som har beviljats status som kvalificerad enligt eIDAS-förordningen före den 20 maj i år, möjlighet att behålla sin status som kvalificerad tillhandahållare på grundval av en rapport om bedömning av överensstämmelse, om rapporten lämnas till tillsynsmyndigheten senast den 21 maj 2026 (artikel 51.4).

Även de redovisade övergångsbestämmelserna är direkt tillämpliga som svensk lag och förutsätter inte att några lagstiftningsåtgärder vidtas.

De författningsförslag som vi lämnar utgör, som framgått, anpassningar av svensk rätt, vilka är föranledda av den reviderade eIDAS-förordningens krav på medlemsstaterna att säkerställa *dels* tillhandahållandet av en europeisk digital identitetsplånbok, *dels* att sanktionsavgifter ska kunna beslutas vid regelöverträdelser som begås av kvalificerade och icke-kvalificerade tillhandahållare av betrodda tjänster.

Det är angeläget att nya och ändrade bestämmelser, i synnerhet förslagen gällande införande av sanktionsavgifter, kan träda i kraft så snart som möjligt. Utifrån gällande beredningskrav i lagstiftningsärenden är det dock, enligt vår bedömning, inte realistiskt med ett ikraftträdande förrän den 1 oktober 2025.

De i förordningen föreskrivna kraven om och kopplade till tillhandahållandet av den europeiska digitala identitetsplånboken, som enligt våra förslag ska åvila vissa av regeringen utsedda myndigheter, medför ett omfattande utvecklings- och omställningsarbete för berörda myndigheter. Detsamma gäller även för alla övriga aktörer som omfattas av den reviderade eIDAS-förordningens tillämpningsområde. Av förordningen framgår dock att dessa krav ska uppfyllas av medlemsstaterna och övriga berörda aktörer inom 24 månader efter ikraftträdande av kommissionens genomförandeakter (med bl.a. referensstandarder för identitetsplånboken och dess certifiering), som ska antas senast den 21 november 2024. Det innebär att det finns ett visst utrymme för att vidta de åtgärder som föreskrivs i förordningen och föreslagna kompletterande svenska bestämmelser.

Någon motsvarande tidsförskjutning gäller inte avseende kravet om sanktionsavgifter. Vi har övervägt men inte funnit tillräckliga skäl

för att föreslå olika tidpunkter för ikraftträdande av föreslagna författningsändringar.

En övergångsbestämmelse behövs med anledning av förslagen om ändrad och ny reglering avseende ingripanden vid regelöverträdelser.

Av 2 kap. 10 § regeringsformen följer ett förbud mot retroaktiv straff- och skattelagstiftning. Förbudet omfattar formellt inte administrativa sanktioner, men anses analogivis tillämpligt beträffande straffliknande administrativa påföljder.² De nya bestämmelserna om administrativa sanktionsavgifter bör således få beslutas endast för överträdelser som har skett efter att bestämmelserna trätt i kraft. Det bör därför uttryckligen framgå att nuvarande bestämmelser fortfarande ska gälla för överträdelser som har ägt rum före ikraftträdandet.

² prop. 1975/76:209 s. 125.

8 Konsekvenser

8.1 Inledning

I slutbetänkandet redovisas våra förslag som avser nödvändiga anpassningar till den reviderade eIDAS-förordningen.

I detta kapitel redogör vi för förslagets effekter i den omfattning som bedömts lämpligt och med beaktande av relevanta delar av kommittéförordningen (1998:1474) och den numera upphävda förordningen (2007:1244) om konsekvensutredning vid regelgivning.¹ För våra överväganden om behov av integritetsskydd med anledning av lämnade förslag hänvisas till avsnitt 6.3.9 tillsammans med avsnitt 6.8 och 6.9 i tillämpliga delar.

8.2 Konsekvenser av den reviderade eIDAS-förordningen

Denna konsekvensanalys omfattar konsekvenserna av våra förslag. Trots att det inte utgör en del av vårt uppdrag redovisas även översiktligt i detta avsnitt vissa konsekvenser som den reviderade eIDAS-förordningen innebär. Vi har även gett Governo AB i uppdrag att utreda och analysera

- Vilka aktörer som berörs av kravet i bilaga VI till den reviderade eIDAS-förordningen som fastställer vilka attributsintyg som varje medlemsland som ett minimum ska utfärda, och

¹ Förordningen (2007:1244) om konsekvensutredning vid regelgivning har numera upphävts och ersatts av förordningen (2024:183) om konsekvensutredningar som trädde i kraft den 6 maj 2024. Av övergångsbestämmelserna framgår emellertid att förordningen inte ska tillämpas för kommittéer och särskilda utredare som tillkallats före ikraftträdandet och att 6 och 7 §§ i den upphävda förordningen om konsekvensutredning vid regelgivning då ska tillämpas.

- uppskatta kostnader för utfärdande av attributsintyg för offentliga aktörer och kostnad för att validera attributsintyg utfärdade av kvalificerade tillhandahållare av betrodda tjänster.

Governo AB redovisade sitt uppdrag den 31 maj 2024 och med beaktande av de snäva tidsramar som råder redovisas inte dessa konsekvenser av den reviderade eIDAS-förordningen här, rapporten fogas dock som en bilaga till betänkandet (se bilaga 4).

Vad gäller mer övergripande konsekvenser av den reviderade eIDAS-förordningen har kommissionen gjort en konsekvensanalys av sitt ursprungliga förslag.² Konsekvensbedömningen, som alltså redovisades 2021, är både kvantitativ och kvalitativ och visar att de lägsta kvantifierbara kostnaderna kan uppskattas till ungefär 3,2 miljarder euro.³ De totala kvantifierbara fördelarna uppskattades till mellan 3,9 miljarder euro och 9,6 miljarder euro.⁴

När det gäller de bredare ekonomiska effekterna förväntades det alternativ som förordades av kommissionen – och som i väsentliga delar motsvarar den antagna förordningens omfattning – ha en positiv inverkan på innovation, internationell handel och konkurrenskraft samt bidra till ekonomisk tillväxt och leda till ytterligare investeringar i lösningar för digital identitet.

Kommissionen bedömde att de totala finansiella resurser som krävs för genomförandet av förslaget under perioden 2022–2027 kommer att uppgå till 30,825 miljarder euro, inklusive 8,825 miljarder euro i administrativa kostnader och upp till 22 miljarder euro i driftskostnader.⁵ Kostnaderna förväntades täckas av Programmet för det digitala Europa.⁶

Finansieringen avser kostnader i samband med underhåll, utveckling, drift och stöd till byggblocken för e-legitimation och betrodda tjänster. Programmet för det digitala Europa kan också ge stöd till anslutning av tjänster till ekosystemet för den europeiska digitala

² European Commission, *Commission staff working document, Impact Assessment Report, Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) no 910/2014 as regards establishing a framework for a European Digital Identity*, COM(2021)124 final.

³ European Commission, a.a., s. 57.

⁴ European Commission, a.a., s. 59.

⁵ European Commission, a.a., s. 57.

⁶ Programmet pågår under 2021–2027 med en totalbudget på 7,6 miljarder euro och syftar till att bygga digital kapacitet och infrastruktur inom EU med fokus på att underlätta bred användning av digital teknik och sätta resultat från forskning på marknaden. Läs mer om programmet på www.digg.se/ledning-och-samordning/programmet-for-ett-digitalt-europa (hämtad 2024-05-26).

identitetsplånboken, utveckling av standarder och tekniska specifikationer. Kommissionen har publicerat en finansieringsöversikt för detta initiativ med en detaljerad översikt över kostnaderna.⁷

Konsekvenserna för nationella budgetar påverkas enligt kommissionen av:

- Krav på att anmäla en e-legitimation för de medlemsstater som inte har anmält en sådan.
- Kostnader som är direkt kopplade till anmälningsförfarandet.
- Kostnader för att tillgängliggöra digitala bevis.
- Kostnader för att utveckla och underhålla en digital identitetsplånbok.
- Kostnader i samband med t.ex. standardisering, certifiering, regel efterlevnad och tillsyn av nya betrodda tjänster.

Regeringen har tidigare bedömt att det 2021 inte var fullt ut möjligt att förutse eventuella budgetära konsekvenser för svensk del. Samtidigt konstaterades att en ökad användning av digitala tjänster samt ökad konkurrens medför samhällsekonomiska vinster och i längden kostnadsbesparingar för såväl offentlig som privat sektor.⁸ Särskilt kommer individer och företag som är i behov av gränsöverskridande tjänster att få fördelar även om vissa företag också kommer att få mindre kostnader för att utveckla tjänster som kan hantera användning av identitetsplånboken och digitala bevis. Kommissionen har inte presenterat någon jämförelseanalys.

Den reviderade eIDAS-förordningen kommer att ha konsekvenser för kommuner och regioner genom bl.a. de attributsintyg som både minimiförteckningen i Bilaga VI anger samt invånarnas förväntningar om att identitetsplånböckerna ska förses med attributsintyg som har sitt ursprung i kommun- och regionsektorn.

Vad gäller företag ställer förordningen bl.a. krav på att företag inom vissa sektorer och tjänster som kräver stark autentisering ska godta identitetsplånböcker.

Våra bedömningar kring identitetsplånbokens användningsområden för nationell effektivitet och nytta framgår av avsnitt 6.8 och i

⁷ A.a., s. 52.

⁸ Regeringskansliet, Faktapromemoria 2020/21:FPM118.

avsnitt 6.9 redogörs för identitetsplånbokens konsekvenser för brottsligheten och det brottsförebyggande arbetet.

8.3 Nollalternativ

En beskrivning av nollalternativ innefattar en bedömning av vad som händer om de föreslagna åtgärderna inte genomförs. Alla medlemsstater är skyldiga att följa förordningen och vidta åtgärder för att densamma ska få fullt genomslag. Underlåtenhet att vidta erforderliga åtgärder skulle innebära att Sverige blir föremål för ett överträdelseärende.

8.4 Vilka myndigheter berörs av förslagen?

De myndigheter som främst berörs av förslagen är Myndigheten för digital förvaltning (Digg), Post- och telestyrelsen (PTS), Bolagsverket och Försvarets materielverk (FMV). För FMV bedöms dock förslagen leda till begränsade konsekvenser som inte kräver finansiering i särskild ordning. Om arbetet med att utse ett certifieringsorgan innebär att FMV behöver inta en mer aktiv roll alternativt själva behöver tillhandahålla certifieringen innebär det emellertid avsevärt högre kostnader för myndigheten. Ett visst utlämnande av uppgifter från Statistiska centralbyrån kommer att behöva ske för att Bolagsverket ska kunna tillhandahålla personidentifieringsuppgifter för vissa juridiska personer (LPID). Det bedöms dock inte röra sig om uppgiftsöverlämning av sådan omfattning att det kräver finansiering i särskild ordning.

8.5 Förslaget om ansvar för tillhandahållande av en identitetsplånbok

Vi föreslår en öppen modell för tillhandahållande av en europeisk digital identitetsplånbok vilket gör det möjligt för både offentliga och privata aktörer att tillhandahålla sådana identitetsplånböcker. Det är inte säkert att privata aktörer väljer att tillhandahålla identitetsplånböcker och för att identitetsplånböcker ska vara tillgängliga för fysiska och juridiska personer inom den tidsram som förordningen kräver behöver en offentlig aktör tillhandahålla dem. Vi har gjort bedömningen

att Digg är bäst lämpad att tillhandahålla europeiska digitala identitetsplånböcker för både fysiska och juridiska personer.

Digg har i sitt budgetunderlag för åren 2025–2027 uppskattat myndighetens kostnader för att tillhandahålla en identitetsplånbok.⁹

Digg har i budgetunderlaget utgått från den konsekvensutredning som EU-kommissionen tog fram i samband med att förslaget till revidering av eIDAS-förordningen lämnades.¹⁰ Det finns i nuläget många osäkra faktorer och oklarheter avseende hur identitetsplånböckerna tekniskt ska fungera och därmed vilka kostnader som följer av att tillhandahålla en europeisk digital identitetsplånbok. Det beror på att flera av förutsättningarna för den tekniska utformningen av identitetsplånböcker, certifiering för identitetsplånböcker, förteckningar över tillhandahållare och valideringsmekanismer inte kommer att vara klara förrän de genomförandeakter som ska tas fram till i slutet av år 2024 har publicerats. Detta medför att alla kostnader inte går att uppskatta och att det finns osäkerheter rörande nedan presenterade beräkningar. Vad gäller kostnader som inte omfattas av Diggs budgetunderlag har utredningen fört en dialog med berörda aktörer samt i vissa fall gjort egna uppskattningar.

Tabell 8.1 Uppskattade årliga kostnader för att ta fram och tillhandahålla identitetsplånbok från Diggs budgetunderlag för åren 2025–2027

	2025	2026	2027
Utveckling av identitetsplånboken	7 mnkr	10 mnkr	9 mnkr
Drift, förvaltning och vidareutveckling av identitetsplånboken	19 mnkr	25 mnkr	51 mnkr
Totalt finansieringsbehov	26 mnkr	35 mnkr	60 mnkr

⁹ Myndigheten för digital förvaltning, Budgetunderlag 2025–2027, 2024-03-01, Diarienummer 2024-0931.

¹⁰ Commission staff working document, Impact Assessment Report, Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) no 910/2014 as regards establishing a framework for a European Digital Identity, COM(2021)124 final.

8.5.1 Övriga tillkommande kostnader för att tillhandahålla identitetsplån-boken

Tillhandahållande av identitetsplån-bok för juridiska personer

En identitetsplån-bok för juridiska personer skiljer sig till viss del från en identitetsplån-bok för fysiska personer. Vid användning av plån-böcker för juridiska personer är det troligen mer intressant för dessa att anskaffa en serverbaserad identitetsplån-bok än en applikation i en mobiltelefon. Det innebär att det åtminstone kommer att behöva göras anpassningar av identitetsplån-boken då den framför allt är avsedd för användning av privatpersoner. Beräkningarna nedan utgår från att LPID hämtas från Bolagsverket till identitetsplån-boken och inte anpassning av plån-boken för juridiska personer.

Tabell 8.2 Kostnad för att hämta LPID till identitetsplån-boken

	2025	2026	2027
Utveckling av tjänst för att hämta LPID från Bolagsverket	4,5–7,5 mnkr	3,5–6,5 mnkr	
Drift, förvaltning och vidareutveckling av tjänsten (årlig)			7,5 mnkr/år

Förteckningar över tillhandahållna och godkända identitetsplån-böcker och PID

I kostnaderna ingår utveckling, drift och förvaltning av förteckningar över de identitetsplån-böcker som tillhandahålls eller godkänns och över utfärdare av personidentifieringsuppgifter (PID).

Tabell 8.3 Förteckning över identitetsplån-böcker och PID

	2025	2026	2027
Utveckling av förteckningar över plån-böcker och PID	9–15 mnkr	7–13 mnkr	
Drift, förvaltning och vidareutveckling (årlig)			13–15 mnkr/år

Kostnadsfri valideringsmekanism

I detta fall handlar det om den kostnadsfria valideringsmekanismen för kontroll av plånböckers äkthet och giltighet. Uppskattningen avser kostnaden för validering av en statligt tillhandahållen plånbok.

Tabell 8.4 Kostnadsfri valideringsmekanism

	2025	2026	2027
Utveckling av tjänst för att kontrollera en identitetsplånboksinstans äkthet mot relevanta register	6–10 mnkr	4–8 mnkr	
Drift, förvaltning och vidareutveckling av tjänsten (årlig)			11,5–12,5 mnkr/år

Kostnader för certifiering

Kostnaderna avser arbete med certifieringsordningar på både nationell och EU-nivå. Kostnader avser även certifiering av en plånbokslösning och att upprätthålla certifieringen.

Tabell 8.5 Kostnader för certifiering

	2024	2025	2026	2027
Utveckling av certifieringsordningar	2–3 mnkr	2–3 mnkr	2–3 mnkr	2–3 mnkr
Första certifiering av identitetsplånbokslösning			6 mnkr	
Årlig kostnad för att uppfylla certifieringskrav				2,5 mnkr/år

Utöver dessa kostnader finns flera andra möjliga kostnader som kan hänföras till de kommande genomförandeakterna och till de tekniska val som görs och hur användningen kommer att bli. Det handlar t.ex. om särskilda behov som uppstår gällande användning av identitetsplånböcker för juridiska personer. Det handlar också om att identitetsplånboken ska kunna användas för att skapa kvalificerade elektroniska underskrifter. Detta kan ske på flera olika sätt, exempelvis genom att tillhandahålla en sådan kvalificerad betrodd tjänst eller att plånboken används som ett medel för elektronisk identifiering på nivå hög och

används för att få ett kvalificerat certifikat utfärdat av en befintlig kvalificerad betrodd tjänst. En kostnadsberäkning för att tillhandahålla en tjänst för skapande av kvalificerade elektroniska underskrifter gjordes i utredningens delbetänkande.¹¹ Denna beräkning pekade på en uppstartskostnad om cirka 25 miljoner kronor. Om identitetsplån-boken används för att identifiera sig till annans kvalificerade betrodda tjänst föranleder det inga kostnader för tillhandahållaren av identitets-plån-boken.

Totala kostnader för Digg

I tabellen nedan redovisas den totala beräknade kostnaden för de uppgifter vi föreslår att Digg ges.

Tabell 8.6 Totala kostnader för Digg för att tillhandahålla identitetsplånböcker

	2025	2026	2027
Utveckling av identitetsplån-boken	7 mnkr	10 mnkr	9 mnkr
Drift, förvaltning och vidareutveckling av identitetsplån-boken	19 mnkr	25 mnkr	51 mnkr
Hämtning av LPID	4,5–7,5 mnkr	3,5–6,5 mnkr	6,5–7,5 mnkr
Förteckningar över identitetsplånböcker och PID	9–15 mnkr	7–13 mnkr	13–15 mnkr
Kostnadsfri valideringsmekanism för identitetsplån-boken	6–10 mnkr	4–8 mnkr	11,5–12,5 mnkr
Certifieringskostnader	2–3 mnkr	8–9 mnkr	4,5–5,5 mnkr
Totalt finansieringsbehov	47,5–61,5 mnkr	57,5–71,5 mnkr	95,5–100,5 mnkr

Kostnader för att tillhandahålla digitala identitetsplånböcker och PID till fysiska personer får enligt den reviderade eIDAS-förordningen inte avgiftsfinansieras eftersom det ska vara avgiftsfritt för fysiska personer att skaffa, använda eller återkalla digitala identitetsplånböcker. Det medför att tillhandahållandet behöver anslagsfinansieras vad gäller tillhandahållande till fysiska personer. När det gäller juridiska personer ges Digg rätt att ta ut avgifter. Detta bedöms emellertid endast ge viss kostnadstäckning och intäkterna lär även variera över tid.

¹¹ *En säker och tillgänglig statlig e-legitimation* (SOU 2023:61), s. 142.

8.5.2 Förslaget om att tillhandahålla personidentifieringsuppgifter för fysiska personer

PID är en förutsättning för att en europeisk digital identitetsplånbok ska kunna användas som medel för elektronisk identifiering. Vi bedömer att Digg är bäst lämpad att tillhandahålla PID. I tillhandahållandet av PID ingår att:

- verifiera identiteten hos en användare av den digitala identitetsplånboken i enlighet med kraven för tillitsnivå hög,
- utfärda PID till den digitala identitetsplånboken i ett harmoniserat gemensamt format, och
- göra information tillgänglig för förlitande parter för att möjliggöra validering av PID.

Den exakta utformningen av PID och eventuella begränsningar i den möjliga uppbyggnaden och utformningen av PID kommer att styras av den genomförandeakt enligt artikel 5a.23 som kommissionen ska ta fram till senast den 21 november 2024. Detta medför att precisa uppskattningar av kostnaderna är svåra att göra. För att tillhandahålla PID kommer det att krävas uppbyggnad och anpassning av Diggs verksamhet. Om lämnade förslag om statlig e-legitimation genomförs och Digg utses till utfärdare kan det vara möjligt att samhantera utfärdande av den statliga e-legitimationen och tillhandahållande av PID för fysiska personer. Digg har, i sådant fall, i egenskap av ansvarig för den föreslagna databasen över statliga e-legitimationer, tillgång till nödvändiga uppgifter för att tillhandahålla PID för fysiska personer vilket skulle kunna sänka kostnaden för denna hantering. Om förslaget om den statliga e-legitimationen inte genomförs kan Digg enligt 2 kap. 8 § första stycket lagen (2001:182) om behandling av personuppgifter i Skatteverkets folkbokföringsverksamhet medges direktåtkomst till uppgift om bl.a. person- och samordningsnummer, namn, adress och avregistrering från folkbokföringen.

Vi har bedömt resursbehovet för att tillhandahålla PID till utvecklingskostnader om 30 miljoner kronor och därefter årliga drift- och förvaltningskostnader om 10 miljoner kronor per år.

Tabell 8.7 Tillhandahålla PID för fysiska personer

	2025	2026	2027
Utveckling av identitetsverifiering, koppling till Navet m.m.	15 mnkr	15 mnkr	
Drift, förvaltning och vidareutveckling (årlig)			10 mnkr/år

8.5.3 Förslaget om att tillhandahålla personidentifieringsuppgifter för juridiska personer

Vi bedömer att Bolagsverket är bäst lämpad att tillhandahålla LPID. För att kunna tillhandahålla LPID kommer det att krävas förändringar i Bolagsverkets it-miljö, bl.a. för att hantera e-legitimationer på högsta tillitsnivån. Det tillkommer även administrativa kostnader för att vara en utfärdare av LPID. Bolagsverket gör bedömningen att den totala utvecklingskostnaden är 15 miljoner kronor och därefter en årlig kostnad om 6 miljoner kronor per år för drift och förvaltning av utfärdandeprocessen av LPID. I kostnaderna ingår:

- Inloggning med högsta tillitsnivå och med identitetsplånbok
- Kvalificerad elektronisk underskrift (även med identitetsplånbok)
- Betalning (med utgångspunkten stöd för betalning via identitetsplånbok)
- Diarieföring
- Ärendehantering
- Kundservice
- Integration mot andra myndigheter för en samlad process
- Granskning, eventuell certifiering och tillkommande administration (inkluderade registrering på en förteckning för tillhandahållare av PID).

Uppbyggnaden av verksamheten och utvecklingen av system för att tillhandahålla identitetsplånboken behöver anslagsfinansieras. Därefter kan delar av driften avgiftsfinansieras genom en ansökningsavgift för den som ansöker om LPID. Dessa avgifter kommer dock att

variera över tid och kommer inte att till fullo kunna finansiera driftskostnaderna.

8.6 Förslaget om tillsyn över identitetsplånboken och förändrad tillsyn över betrodda tjänster

PTS är för närvarande tillsynsmyndighet över tillhandahållare av betrodda tjänster och de betrodda tjänster som tillhandahålls. Tillsyn av plånboken påminner till viss del om tillsyn över kvalificerade tillhandahållare av betrodda tjänster eftersom det sker en förhandsgranskning av certifieringsorgan som granskar tillhandahållare och tjänst innan de kan börja tillhandahålla tjänster. Rapporter om överensstämelsebedömning är ett viktigt verktyg i tillsynen. Tillsyn över identitetsplånboken är däremot ett nytt område för PTS som kommer att kräva kompetensuppbyggnad. I rollen ingår även att granska och vidta åtgärder mot förlitande parter vid misstänkt olagligt eller bedrägligt beteende.

Antalet potentiella tillhandahållare av identitetsplånböcker som tillhandahålls eller erkänns i Sverige bedöms bli få till antalet varför resursbehovet av PTS har bedömts vara begränsat. Däremot medför det faktum att det är ett nytt område, samt det faktum att antalet tillhandahållare av kvalificerade och icke-kvalificerade betrodda tjänster bedöms öka, finnas ett behov av resursförstärkning. Förändringen av antalet tillhandahållare av betrodda tjänster hänger främst samman med det stora potentiella antalet tillhandahållare som kan komma att tillhandahålla attributsintyg. PTS har i dag en finansiering om 3 miljoner kronor via anslag och rätt att ta ut avgifter. Det är totalt tre årsarbetskrafter som arbetar med tillsynen av betrodda tjänster i dagsläget.

PTS har i dialog med utredningen bedömt att de kommer att behöva totalt 8–10 årsarbetskrafter för den kommande utökade tillsynen med ansvar för tillsyn över identitetsplånböcker. Det skulle innebära totalt finansieringsbehov om 8–10 miljoner kronor per år. Avgiftsfinansiering kan användas till viss del för kostnadstäckning, men huvuddelen av finansieringen bedöms behöva ske via anslag. PTS tar för närvarande ut en årsavgift för kvalificerade tillhandahållare av betrodda tjänster om 25 000 kronor per år. Dessa avgifter bidrar med kostnadstäckning även om antalet kvalificerade tillhandahållare av

betrodda tjänster blir fler kommer inte avgifterna innebära mer än begränsad kostnadstäckning för PTS verksamhet på området. Om exempelvis 10 nya aktörer etablerar sig bidrar avgifterna med endast 250 000 kronor per år.

8.7 Förslaget om att tillhandahålla registret över förlitande parter

PTS föreslås ansvara för registret över förlitande parter. PTS har i dialog med utredningen redogjort för bedömningar av vilka konsekvenser ett sådant uppdrag skulle medföra för myndigheten. Registret kommer att vara en del av infrastrukturen och kommer att behöva vara tillgängligt för att det ska gå att använda identitetsplånböckerna. Registret kommer att innehålla många förlitande parter, BankID nås t.ex. av i storleksordningen 7 100 förlitande parter i Sverige.¹² Målet med identitetsplånböckerna är att nå fler förlitande parter än dagens e-legitimationssystem. Uppgifter om förlitande parter kommer att behöva uppdateras ofta och vara korrekta, vilket medför att det kommer att behöva göras av den förlitande parten själv. Ett system för detta behöver utvecklas, förvaltas och vidareutvecklas. Utformningen av registret kommer även påverkas av de genomförandeakter som EU-kommissionen ska ta fram till slutet av år 2024 och det är först då som de praktiska förutsättningarna för registret är kända.

PTS har i nuläget inget ansvar som omfattar att tillhandahålla infrastruktur eller system med höga krav på tillgänglighet. PTS har i dagsläget inte heller kompetens att hantera ett sådant register utifrån teknisk- och administrativ erfarenhet, driftställen, säkerhetsnivå och jourverksamhet m.m. PTS bedömer att lösningen kommer behöva upphandlas av en eller flera säkra underleverantörer som besitter kompetens och erfarenhet av stora datamängder samt hantering av hot och förändring i liknande register. Trots upphandling kommer PTS egna personal behöva vara en aktiv kravställare och involveras som ansvarig för registret. Det gör att viss typ av jourverksamhet är oundviklig för att det ska finnas aktiva och fungerande kontaktpunkter. Kostnaderna för att tillhandahålla registret skulle enligt PTS möjligen kunna vara lägre om det tillhandahölls av en aktör som har vana vid den här typen av utvecklingsuppdrag och drift.

¹² www.bankid.com/om-oss/press (hämtad 2024-05-26).

Vidare kan det tillkomma kostnader för att tillhandahålla valideringsmekanism som möjliggör för användare av identitetsplånböcker att kontrollera förlitande parter som förekommer i registret om inte funktionaliteten för detta är inbyggd i identitetsplånboken.

Tabell 8.8 PTS bedömning av kostnader för registret för förlitande parter

	2025	2026	2027
Utveckling och införande kostnader	2,5 mnkr	2,5 mnkr	
Drift- och förvaltningskostnader			7,5 mnkr per år
Övriga kostnader som personal-kostnader, användarstöd och systemförvaltning			2,5 mnkr per år
Totalkostnad	2,5 mnkr	2,5 mnkr	10 mnkr

8.8 Konsekvenser för offentlig sektor i övrigt

8.8.1 Konsekvenser för domstolarna

Våra förslag kan föranleda att tillsynsmyndigheten över europeiska digitala identitetsplånböcker samt övriga utpekade myndigheter fattar beslut enligt den reviderade eIDAS-förordningen med tillhörande genomförandeakter och kompletterande svenska författningar. Sådana beslut får överklagas till allmän förvaltningsdomstol. Med hänsyn till att endast ett begränsat antal beslut bedöms fattas sett till det förväntade antalet tillhandahållare kommer reglerna få så begränsad tillämpning att någon ytterligare måltillströmning av betydelse till de allmänna förvaltningsdomstolarna inte är att vänta. Våra förslag bedöms därför inte få några konsekvenser för de allmänna förvaltningsdomstolarna som måste finansieras i särskild ordning.

8.8.2 Kommuner och regioner

Den kommunala självstyrelsen

I 14 kap. 3 § regeringsformen anges att en inskränkning i den kommunala självstyrelsen inte bör gå utöver vad som är nödvändigt med hänsyn till de ändamål som föranlett den. En lagstiftning som ställer upp krav för en kommunal verksamhet minskar generellt sett kom-

munernas möjligheter att själva göra prioriteringar i sin verksamhet. Våra förslag får ingen påverkan på den kommunala självstyrelsen.

Kommunala finansieringsprincipen

Kommunala finansieringsprincipen innebär att om staten inför nya eller ändrade föreskrifter som ändrar skyldigheter för kommunerna och regionerna kan detta påverka dessas kostnader. För att hantera sådana konsekvenser har i samförstånd mellan staten, kommunerna och regionerna en finansieringsordning utvecklats, den s.k. kommunala finansieringsprincipen. Våra förslag innefattar inga nya åtaganden eller skyldigheter för kommunerna och regionerna.

8.9 Konsekvenser för företag

8.9.1 Berörda företag

De förslag som lämnas i betänkandet bedöms ge vissa konsekvenser för framför allt företag som är verksamma inom områdena elektronisk identifiering och betrodda tjänster.

När det gäller utfärdare av e-legitimationer på den svenska marknaden består marknaden i praktiken endast av två e-legitimationer. Dels BankID som ägs av Finansiell ID-Teknik BID AB (Finansiell ID-Teknik), dels Freja+ som ägs av Freja eID Group AB (Freja). Finansiell ID-Teknik hade år 2022 en omsättning på 311 miljoner kronor¹³ och Freja hade år 2023 inom segmentet Freja eID en omsättning på 16,8 miljoner kronor.¹⁴ En mer utförlig redogörelse för dessa bolags verksamhet och e-legitimationer återfinns i vårt delbetänkande.¹⁵

Därtill finns det ett cirka 20 leverantörer som erbjuder olika former av tjänster för elektronisk identifiering och integrationstjänster på den svenska marknaden. Ett fåtal tjänsteleverantörer har dock betydande delar av marknaden. Dessa leverantörer är av varierande storlek. Vissa företag ingår i större it-koncerner, men det finns ett fåtal mikroföretag som också verkar på marknaden.¹⁶

¹³ Årsredovisning för Finansiell ID-Teknik BID AB Räkenskapsåret 2022-01-01 – 2022-12-31.

¹⁴ Årsredovisning och koncernredovisning, Freja eID Group AB, 2023, s. 18.

¹⁵ *En säker och tillgänglig statlig e-legitimation* (SOU 2023:61), s. 77 ff.

¹⁶ *Promemoria om auktorisationssystem för elektronisk identifiering och för digital post*, s. 52.

När det gäller företag verksamma inom området betrodda tjänster utförde Utredningen om betrodda tjänster under hösten 2020 en begränsad marknadsundersökning och PTS gjorde under samma period en undersökning av vilka tillhandahållare av betrodda tjänster som finns på den svenska marknaden.¹⁷ Den sammantagna bilden utifrån dessa undersökningar visade att den svenska marknaden 2020 bestod av cirka 70–80 tillhandahållare av betrodda tjänster. I dagsläget finns det två kvalificerade tillhandahållare, och resterande icke-kvalificerade, tillhandahållare av betrodda tjänster. Dessa tillhandahållare erbjuder olika betrodda tjänster men flera, cirka 45 aktörer erbjuder tjänster med koppling till elektroniska underskrifter. Flera av dessa tillhandahållare erbjuder även möjlighet att validera de underskrifter som levereras inom ramen för deras underskriftstjänst. Några av dessa aktörer är, utöver den svenska marknaden, även aktiva på den nordiska, europeiska eller internationella marknaden.

De utförda marknadsundersökningarna visar att storleken på de företag som tillhandahåller betrodda tjänster på den svenska marknaden varierar kraftigt och innefattar allt från verksamhet med koppling till de stora bankkoncernerna eller stora it-bolag till mellanstora bolag och fåmansföretag.

8.9.2 Påverkan på företag inom området elektronisk identifiering

Den reviderade eIDAS-förordningen kommer på olika sätt påverka företag inom området elektronisk identifiering. Med utgångspunkt i de förslag vi lämnar kommer påverkan framför allt ske genom hur europeiska digitala identitetsplånböcker tillhandahålls.

Vi föreslår en öppen modell för tillhandahållande av identitetsplånböcker som innebär att en privat aktör, efter godkännande, kan tillhandahålla en europeisk digital identitetsplånbok. Detta innebär att befintliga e-legitimationsutfärdare kan tillhandahålla identitetsplånböcker. Det möjliggör även nyetablering på marknaden för både svenska och utländska aktörer.

Vad gäller privata aktörers tillhandahållande har det emellertid från näringslivshåll ifrågasatts om det går att få till en hållbar affärsmodell för detta. Vi delar uppfattningen att det, utifrån vad som i

¹⁷ *Vem kan man lita på? – Enkel och ändamålsenlig användning av betrodda tjänster i den offentliga förvaltningen* (SOU 2021:9) s. 240 f.

skrivande stund är känt om identitetsplån-boken och hur den ska användas, är oklart hur betydande intäkter ska kunna genereras när det gäller identitetsplån-böcker som tillhandahålls privatpersoner. Affärsmodellen för svenska e-legitimationsutfärdare bygger till stor del på att privatpersoners användning av e-legitimationer finansieras genom att det är den förlitande parten som betalar för den identifiering som sker. En sådan konstruktion, där alla europeiska identitetsplån-böcker ska kunna användas gränsöverskridande, är inte möjlig. Utfallet blir därmed detsamma som för de nationella e-legitimationer som anmälts i enlighet med eIDAS-förordningen och som därmed kan användas i alla medlemsstater, men där ingen ersättning utgår till utfärdaren för den användning som sker hos förlitande parter i andra länder. Det har av denna anledning efterfrågats att nationell reglering ska medföra att ersättning för användning hos förlitande parter kan utgå. Någon möjlighet att införa nationella bestämmelser som möjliggör någon form av ersättning till privata tillhandahållare är inte möjlig då detta inte kan anses vara tillåtet enligt eIDAS-förordningen. I fråga om den europeiska digitala identitetsplån-boken är den reglerad på EU-nivå och detta innebär att utrymmet för Sverige och andra medlemsstater att vidta olika typer av åtgärder på området är begränsat till de fall där förordningen medger detta.

När det gäller organisationsplån-böcker finns inte samma begränsningar och det är exempelvis möjligt att ta ut en avgift av det bolag som vill anskaffa en organisationsplån-bok. Samma begränsningar vad gäller löpande intäkter från förlitande parter föreligger dock alltjämt.

Vi föreslår även att en statlig identitetsplån-bok ska tillhandahållas. Detta är en följd av att det föreligger ett krav om att varje stat ska tillhandahålla en europeisk digital identitetsplån-bok. Förordningen tillåter att identitetsplån-boken utfärdas a) direkt av en medlemsstat, b) på uppdrag av en medlemsstat eller c) oberoende av en medlemsstat men erkänd av ifrågavarande medlemsstat (se artikel 5a.2 och skäl 16 i förordningens ingress samt jfr artikel 7 om berättigande till anmälan av system för elektronisk identifiering). För att garantera att identitetsplån-bok tillhandahålls, och då det med beaktande av ovan angivna omständigheterna får anses osäkert om privata aktörer kommer välja att tillhandahålla en identitetsplån-bok, får det anses nödvändigt att den tillhandahålls direkt eller på uppdrag av en statlig myndighet. Förslaget innebär således inte att den tillhandahållande myndigheten kommer att behöva utveckla den tekniska lösningen utan myndigheten

kan välja att upphandla hela eller delar av lösningen från privata aktörer. Detta skapar således möjligheter för företag att erbjuda staten de lösningar de tillhandahåller.

Statens verksamhet att tillhandahålla en identitetsplånbok kommer att utgöra en ekonomisk verksamhet för vilken vissa förfaranden som omfattas av förbudet mot konkurrensbegränsande offentlig verksamhet kommer att vara tillämpliga. Åtgärden får anses försvarbar från allmän synpunkt då tillhandahållandet är en följd av förordningens krav.¹⁸ När det gäller organisationsplånboken föreslås att en avgift tas ut från den juridiska person som önskar en sådan identitetsplånbok. För det fall privata aktörer också tillhandahåller organisationsplånböcker bör hänsyn tas till dessa aktörer så att avgiften för det statliga alternativet inte avviker från privata aktörers avgifter då den statliga tillhandahållaren ska verka på lika villkor som de privata alternativ som finns på marknaden. En utförlig genomgång av de konkurrensrättsliga aspekterna som även här är av relevans återfinns i vårt delbetänkande.¹⁹

Kravet om att tillhandahålla en europeisk digital identitetsplånbok gäller alla EU:s medlemsstater. Vi ser inte att tillhandahållandet utgör en sådan verksamhet som kan påverka konkurrensen och handeln mellan medlemsstaterna. Vår bedömning är därför att reglerna om statsstöd inte blir tillämpliga till följd av vårt förslag i denna del.²⁰

Företag som väljer att tillhandahålla en identitetsplånbok kommer enligt vårt förslag behöva betala en tillsynsavgift. En liknande avgift finns i dag för kvalificerade tillhandahållare av betrodda tjänster. Tillsynsavgiften för dessa aktörer är 25 000 kronor per år. Tillsynsavgiften för identitetsplånböcker kan antas vara på en liknande nivå och är således inte så hög att det ens för mindre företag kan anses utgöra ett hinder för marknadsinträde.

Av förordningen följer att kostnadsfria valideringsmekanismer ska tillhandahållas av medlemsstaterna i syfte att a) säkerställa att europeiska digitala identitetsplånböckers äkthet och giltighet kan kontrolleras och b) göra det möjligt för användare av europeiska digitala identitetsplånböcker att kontrollera äkthet och giltighet för identiteten hos de förlitande parter som registrerats i enlighet med artikel 5 b (artikel 5a.8). Se mer om dessa valideringsmekanismer i avsnitt 6.3.5. Enligt vår bedömning finns det inga bestämmelser i förordningen

¹⁸ Prop. 2008/09:231 s. 37 f.

¹⁹ *En säker och tillgänglig statlig e-legitimation* (SOU 2023:61), s. 202 ff.

²⁰ Se mer om reglerna om statsstöd i a.a. s. 208 f.

som medför att en viss aktör bör tilldelas ansvaret för att tillhandahålla valideringsmekanismerna. För att säkerställa att de angivna mekanismerna kontinuerligt finns tillgängliga för kostnadsfri användning anser vi emellertid att statliga myndigheter ska ansvara för att tillhandahålla dem. Som en del av tillhandahållande av de personidentifieringsuppgifter som ska ingå i identitetsplånboken behöver även sådana uppgifter kunna valideras. Att kostnadsfri validering möjliggörs för förlitande parter kan påverka de e-legitimationsutfärdare och andra aktörer som i dag tar betalt för denna tjänst. Detta är emellertid en direkt följd av förordningen och inte av våra förslag.

8.9.3 Påverkan på företag som tillhandahåller betrodda tjänster

Vårt förslag om att införa en möjlighet att påföra sanktioner mot tillhandahållare av betrodda tjänster kommer att påverka de företag som tillhandahåller sådana tjänster. Risken för att sanktionsavgift tas ut vid i lagen uppräknade överträdelser av regelverket får anses utgöra ett incitament till att följa kraven som ställs upp och därigenom kan konkurrensen på marknaden i högre utsträckning gynnas av att alla följer samma bestämmelser.

8.9.4 Påverkan på övriga företag

Övriga företag kommer i nämnvärd omfattning endast påverkas i den mån de vill få en organisationsplånbok med tillhörande LPID som de enligt förslaget kommer att få avlägga en avgift för.

8.10 Övriga konsekvenser

Förslagen bedöms inte få några nämnvärda konsekvenser för sysselsättningen och offentlig service i olika delar av landet eller för individer och hushåll. Förslagen bedöms inte heller få några konsekvenser för jämställdheten mellan män och kvinnor samt flickor och pojkar. Våra förslag får vidare inga konsekvenser för att nå de integrationspolitiska målen eller för brottsligheten och det brottsförebyggande arbetet. Förslagen bedöms förenliga med EU-rätten.

8.11 Tidpunkten för ikraftträdande och behovet av speciella informationsinsatser

Vi gör bedömningen att förslagen kan genomföras tidigast den 1 oktober 2025.

Vad gäller speciella informationsinsatser framgår följande av skäl 35 i den reviderade eIDAS-förordningen

För att främja spridningen av europeiska digitala identitetsplånböcker och en bredare användning av digitala identiteter bör medlemsstaterna inte bara främja fördelarna med de relevanta tjänsterna, utan bör även, i samarbete med den privata sektorn, forskare och den akademiska världen, utveckla utbildningsprogram som syftar till att stärka de digitala färdigheterna hos sina medborgare och invånare, särskilt för utsatta grupper, såsom personer med funktionsnedsättning och äldre personer. Medlemsstaterna bör också öka medvetenheten om fördelarna och riskerna med europeiska digitala identitetsplånböcker genom informationskampanjer.

Vi ser att tillhandahållandet av en europeisk digital identitetsplånbok kommer att föranleda behov av informationskampanjer. Framför allt i samband med lanseringen.

9 Författningskommentar

9.1 Förslaget till lag om ändring i lagen (2016:561) om kompletterande bestämmelser till EU:s förordning om elektronisk identifiering

Inledande bestämmelser

1 §

Denna lag kompletterar Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (EU:s förordning om elektronisk identifiering).

Termer och uttryck i lagen har samma betydelse som i EU:s förordning om elektronisk identifiering.

Såvitt gäller behandling av personuppgifter kompletterar denna lag Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), här benämnd EU:s dataskyddsförordning.

Vid sådan behandling av personuppgifter som omfattas av EU:s dataskyddsförordning gäller även lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning och föreskrifter som har meddelats i anslutning till den lagen, om inte annat följer av denna lag eller föreskrifter som meddelats i anslutning till lagen.

Av paragrafen framgår lagens primära innehåll och syfte: att komplettera däri angivna EU-rättsakter. I första stycket har den tidigare statiska hänvisningen till EU:s förordning om elektronisk identifiering tagits bort, och hänvisningarna är nu dynamiska, dvs. de avser rättsakten i den vid varje tidpunkt gällande lydelsen. Detta gäller dock inte bestämmelser om sanktionsavgifter som är statiska, se 20 § och kommentaren till den paragrafen.

De nya bestämmelserna i *tredje och fjärde styckena* upplyser om hur förevarande lag förhåller sig till EU:s dataskyddsförordning och lagen med kompletterande bestämmelser till EU:s dataskyddsförordning samt föreskrifter som meddelats i anslutning till sistnämnda författning. Vad som avses med behandling av personuppgifter framgår av artikel 2 i EU:s dataskyddsförordning. Hänvisningar till dataskyddsförordningen är dynamiska.

Övervägandena såvitt avser första stycket finns i avsnitt 6.2, och i övrigt i avsnitt 6.3.9.

Europeisk digital identitetsplånbok

6 §

Regeringen bestämmer vilken myndighet som ska tillhandahålla den europeiska digitala identitetsplånboken i enlighet med artikel 5a.2 i EU:s förordning om elektronisk identifiering (tillhandahållande myndighet).

Den europeiska digitala identitetsplånboken får tillhandahållas även av den som, efter granskning, har godkänts av den tillhandahållande myndigheten (godkänd tillhandahållare).

Enligt paragrafen, som är ny, ska den europeiska digitala identitetsplånboken tillhandahållas av en statlig myndighet, men även privata aktörer får tillhandahålla en sådan identitetsplånbok.

I *första stycket* bemyndigas regeringen att utse den myndighet som ska tillhandahålla identitetsplånboken (tillhandahållande myndighet) i enlighet med Europaparlamentets och rådets förordning (EU) 2024/1183 av den 11 april 2024 om ändring av förordning (EU) nr 910/2014 vad gäller inrättandet av ett europeiskt ramverk för digital identitet, härefter den reviderade eIDAS-förordningen.

Av den reviderade eIDAS-förordningen följer att tillhandahållandet av den europeiska digitala identitetsplånboken kan ske direkt av en medlemsstat, på dess uppdrag eller efter dess godkännande (artikel 5a.2 och skäl 16 i förordningens ingress). Att även privata aktörer tillåts att tillhandahålla den europeiska digitala identitetsplånboken efter granskning och godkännande av den tillhandahållande myndigheten framgår av paragrafens *andra stycke*. I 7 § finns ett föreskriftsbemyndigande avseende villkor för ett sådant godkännande.

Övervägandena redovisas i avsnitt 6.3.1.

7 §

För ett godkännande som avses i 6 § andra stycket krävs att villkoren för den europeiska digitala identitetsplånboken, liksom för att tillhandahålla en sådan, är uppfyllda i enlighet med EU:s förordning om elektronisk identifiering och de rättsakter som meddelats med stöd av förordningen samt denna lag och föreskrifter som meddelats med stöd av lagen.

Om det, efter ett godkännande, finns anledning att anta att villkoren enligt första stycket inte är uppfyllda ska den tillhandahållande myndigheten snarast underrätta den myndighet som avses i 17 § om detta.

Regeringen eller den myndighet regeringen bestämmer ska meddela föreskrifter om villkor för godkännande och om anmälnings- och granskningsförfarandet enligt 6 § andra stycket.

Paragrafen är ny och innehåller bestämmelser om villkor och granskningsförfarande för godkännande av privata aktörer som tillhandahållare av europeiska digitala identitetsplånböcker (godkända tillhandahållare).

Av första stycket framgår att både sådana identitetsplånböcker och den som avser att tillhandahålla dessa ska efterleva krav och skyldigheter enligt den reviderade eIDAS-förordningen och dess genomförandeakter samt kompletterande nationell reglering, som enligt bemyndigandet i tredje stycket ska meddelas på förordnings- eller myndighetsföreskriftsnivå.

Av andra stycket följer att en underrättelse ska göras till tillsynsmyndigheten över den europeiska digitala identitetsplånboken, om det finns anledning att anta att uppställda villkor inte längre är uppfyllda. Det ankommer i sådant fall på tillsynsmyndigheten att vidta erforderliga åtgärder. Tillsynsmyndighetens ansvar och befogenheter framgår av 17–20 §§, se kommentarer till dessa paragrafer.

Övervägandena finns i avsnitt 6.3.1.

8 §

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om:

1. sådana undantag från kravet att tillhandahålla öppen källkod som avses i artikel 5a.3 i EU:s förordning om elektronisk identifiering, och

2. sådana ytterligare funktioner för den europeiska digitala identitetsplånboken som avses i artikel 5a.7 i EU:s förordning om elektronisk identifiering.

Paragrafen, som är ny, delegerar föreskriftsrätt till regeringen eller den myndighet som regeringen bestämmer. Med sådana ytterligare funktioner enligt punkten 2 inbegrips exempelvis interoperabilitet med befintliga nationella e-legitimationer (se skäl 21 i ingressen till den reviderade eIDAS-förordningen).

Övervägandena finns i avsnitt 6.3.2.

9 §

Regeringen bestämmer vilken eller vilka myndigheter som ska tillhandahålla sådana uppgifter för personidentifiering som avses i artikel 3 i EU:s förordning om elektronisk identifiering, och som ska kunna kopplas till den europeiska digitala identitetsplånboken.

Paragrafen är ny och innehåller bemyndigande för regeringen att utse vilken eller vilka myndigheter som ska tillhandahålla sådana uppgifter för personidentifiering som avses i artikel 3 i den reviderade eIDAS-förordningen. Enligt förordningens definition avses ”en uppsättning uppgifter som utfärdas i enlighet med unionsrätten eller nationell rätt, som gör det möjligt att fastställa identiteten på en fysisk eller juridisk person, eller en fysisk person som företräder en annan fysisk person eller en juridisk person” (artikel 3.3). Ifrågavarande uppgifter benämns även PID (”person identification data”) och, specifikt om juridiska personer, LPID (”legal PID”).

Utfärdade PID (och LPID) ska kunna kopplas till en tillhandahållen digital identitetsplånbok (plånboksinstans). Det är först efter en sådan koppling som plånboksinstansen utgör, och kan användas som, en europeisk digital identitetsplånbok.

Övervägandena finns i avsnitt 6.3.3.

Kostnadsfria valideringsmekanismer

10 §

Den statliga myndighet som regeringen bestämmer ska tillhandahålla

1. en kostnadsfri valideringsmekanism som säkerställer att europeiska digitala identitetsplånböckers äkthet och giltighet kan kontrolleras.

2. En kostnadsfri valideringsmekanism som gör det möjligt för användare av europeiska digitala identitetsplånböcker att kontrollera äkthet och giltighet för identiteten hos de förlitande parter som registrerats enligt 17 § 3.

Paragrafen är ny och innehåller bemyndigande för regeringen eller den myndighet som regeringen bestämmer att utse vilken eller vilka myndigheter som ska tillhandahålla sådana valideringsmekanismer som den reviderade eIDAS-förordningen föreskriver.

Funktionen validering definieras i förordningen som ”en process genom vilken det kontrolleras och bekräftas att data i elektronisk form är giltiga i enlighet med förordningen” (artikel 3.41).

Övervägandena redovisas i avsnitt 6.3.5.

Behandling av personuppgifter för tillhandahållande och återkallelse av den europeiska digitala identitetsplånboken

11 §

Den tillhandahållande myndigheten ska med hjälp av automatiserad behandling föra en databas med en samling uppgifter om de europeiska digitala identitetsplånböcker som myndigheten har tillhandahållit.

Regeringen eller den myndighet som regeringen bestämmer får med stöd av 8 kap. 7 § regeringsformen meddela ytterligare föreskrifter om vilka uppgifter databasen ska innehålla och den längsta tid som personuppgifter får behandlas i databasen.

Paragrafen, som är ny, reglerar den databas över de europeiska digitala identitetsplånböcker som förs av den tillhandahållande myndigheten. I *andra stycket* finns en upplysning om föreskriftsrätt om databasens innehåll.

Övervägandena finns i avsnitt 6.3.9.

12 §

Den tillhandahållande myndigheten får behandla personuppgifter om det är nödvändigt för att handlägga ärenden om tillhandahållande och återkallelse av giltigheten av en europeisk digital identitetsplånbok samt nödvändig administration av databasen över europeiska digitala identitetsplånböcker.

Personuppgifter som avses i första stycket får också behandlas om det är nödvändigt för att fullgöra uppgiftsutlämnande som sker i överensstämmelse med lag eller förordning.

Paragrafen är ny. I *första stycket* anges de ändamål för vilka personuppgifter får behandlas. Bestämmelsen omfattar all nödvändig behandling av personuppgifter i verksamheten med tillhandahållandet av

den europeiska digitala identitetsplånboken, och inte endast den som sker i den databas som myndigheten har rätt att föra.

Av *andra stycket* framgår att behandling av sådana personuppgifter som avses i första stycket får vidarebehandlas, om det behövs för att fullgöra uppgiftsutlämnande som sker i överensstämmelse med lag eller förordning. Det ska alltså vara fråga om författning som antingen påbjuder eller tillåter utlämnande. Bestämmelser om uppgiftsutlämnande finns t.ex. i 6 kap. 5 § offentlighets- och sekretesslagen (2009:400). Den bestämmelsen innehåller en allmän skyldighet för en myndighet att på begäran av en annan myndighet lämna ut uppgifter som inte omfattas av sekretess, förutsatt att det inte skulle hindra arbetets behöriga gång.

Övervägandena redovisas i avsnitt 6.3.9.

13 §

Uppgifter om lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden får inte användas som sökbegrepp i över europeiska digitala identitetsplånböcker.

Regeringen eller den myndighet som regeringen bestämmer får med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om integritetshöjande åtgärder till skydd för personuppgifter i verksamheten med tillhandahållandet av den europeiska digitala identitetsplånboken.

Paragrafen är ny. *Första stycket* innehåller ett sökförbud beträffande uppgifter kopplade till lagöverträdelser och liknande.

I *andra stycket* finns en upplysning om föreskriftsrätt i form av verkställighetsföreskrifter rörande närmare reglering av integritetshöjande åtgärder till skydd för personuppgifter. Det finns alltså ett utrymme att meddela föreskrifter om andra integritetshöjande åtgärder än den som framgår av första stycket.

Övervägandena finns i avsnitt 6.3.9.

14 §

Artikel 21.1 i EU:s dataskyddsförordning om rätten att göra invändningar gäller inte vid sådan behandling av personuppgifter som är tillåten enligt denna lag eller föreskrifter som meddelats i anslutning till lagen.

Paragrafen, som är ny, innehåller en begränsning av den registrerades rätt att göra invändningar enligt artikel 21.1 i EU:s dataskyddsförordning, som är gjord med stöd av artikel 23 i nämnda förordning.

Vid sådan behandling av personuppgifter som är tillåten enligt lagen eller föreskrifter som har meddelats i anslutning till den gäller alltså inte rätten att göra invändningar enligt dataskyddsförordningen. Bestämmelsen omfattar all behandling av personuppgifter som är tillåten enligt lagen, eller föreskrifter som meddelas i anslutning till lagen, och inte endast personuppgiftsbehandling som sker i den databas som avses i 11 §.

Övervägandena finns i avsnitt 6.3.9.

Certifiering

15 §

Regeringen eller den myndighet som regeringen bestämmer ska utse ansvarigt organ för certifiering av europeiska digitala identitetsplånböcker, system för elektronisk identifiering, anordningar för skapande av kvalificerade elektroniska underskrifter och anordningar för skapande av kvalificerade elektroniska stämplor.

Paragrafen är ny och innehåller bemyndigande för regeringen eller den myndighet som regeringen bestämmer att utse ett ansvarigt organ för certifiering av europeiska digitala identitetsplånböcker, system för elektronisk identifiering, anordningar för skapande av kvalificerade elektroniska underskrifter och anordningar för skapande av kvalificerade elektroniska stämplor.

Övervägandena finns i avsnitten 6.3.7 och 6.5.3.

Tillsyn

17 §

Den myndighet som regeringen bestämmer (tillsynsmyndigheten) ska

1. fullgöra tillsynsorganets uppgifter enligt EU:s förordning om elektronisk identifiering och rättsakter som har meddelats med stöd av den förordningen, och

2. utöva tillsyn över efterlevnaden av denna lag och föreskrifter som har meddelats med stöd av lagen,

3. upprätta, underhålla och offentliggöra en förteckning över förlitande parter och uppgifter om dessa i enlighet med artikel 5b.2 och 5b.5 i EU:s förordning om elektronisk identifiering, och

4. vidta nödvändiga åtgärder i enlighet med artikel 5e.1–3 i EU:s förordning om elektronisk identifiering vid säkerhetsincidenter som rör i artikeln angivna europeiska digitala identitetsplånböcker, valideringsmekanismer eller det system för elektronisk identifiering inom ramen för vilket de europeiska digitala identitetsplånböckerna tillhandahålls.

Tillsynsmyndigheten får meddela föreskrifter om sådana arrangemang och förfaranden för ömsesidigt bestånd som avses i artikel 46d i EU:s förordning om elektronisk identifiering.

Paragrafen reglerar tillsynsmyndighetens uppgifter. *Punkterna 1 och 2 motsvarar bestämmelsen i den tidigare 4 §.*

Tillsynsmyndighetens ansvarsområde omfattar, genom den reviderade eIDAS-förordningen, även tillsyn över att tillhandahållare av europeiska digitala identitetsplånböcker som är etablerade i Sverige efterlever dels kraven i nämnda förordning och de rättsakter som har meddelats med stöd av densamma, dels kraven i denna lag och den förordning och de föreskrifter som har meddelats med stöd av lagen.

Enligt artikel 5b.1 i den reviderade eIDAS-förordningen ska den fysiska eller juridiska person som avser att förlita sig på europeiska digitala identitetsplånböcker för tillhandahållande av offentliga eller privata tjänster genom digital interaktion registrera sig i den medlemsstat där den är etablerad. Av paragrafens nya *punkt 3* följer att tillsynsmyndigheten ska upprätta, underhålla och offentliggöra en förteckning över sådana förlitande parter och uppgifter om dessa i enlighet med artikel 5b.2 och 5b.5 i den reviderade eIDAS-förordningen. Registreringen ska enligt förordningen underlätta medlemsstaternas kontroller av lagenligheten hos de förlitande parternas verksamhet i enlighet med unionsrätten och syfta till att öka öppenheten i och förtroendet för användningen av europeiska digitala identitetsplånböcker.

Enligt den nya *punkten 4* ska tillsynsmyndigheten, vid säkerhetsincidenter, vidta åtgärder i enlighet med artikel 5e. 1–3 i den reviderade eIDAS-förordningen. De åtgärder som, beroende på incidentens allvarsgrad, kan aktualiseras är att tillhandahållandet och användningen av berörda identitetsplånböcker kan bli föremål för tillfälligt upphörande eller permanent återkallelse. Vid ett tillfälligt upphävande ska säkerhetsincidenten åtgärdas inom tre månader, annars ska identitetsplånböckerna återkallas och giltigheten upphävas. I motsatt fall ska tillhandahållandet och användningen i stället återupprättas.

I den nya *punkten 5* ges ett bemyndigande för tillsynsmyndigheten att meddela föreskrifter om arrangemang och förfaranden för gemensamma åtgärder i anslutning till ömsesidigt bistånd som regleras i artikel 46d.

Övervägandena finns i avsnitten 6.6.2–6.6.4.

19 §

Tillsynsmyndigheten får meddela de förelägganden och förbud som behövs för efterlevnaden av

1. EU:s förordning om elektronisk identifiering och rättsakter som har meddelats med stöd av den förordningen, och

2. denna lag och föreskrifter som har meddelats med stöd av lagen.

Förelägganden och förbud *som riktas mot tillhandahållare av betrodda tjänster* får förenas med vite.

Tillsynsmyndigheten får bestämma att beslut enligt första stycket ska gälla omedelbart.

I paragrafen, som tidigare betecknades 6 §, anges de befogenheter som tillsynsmyndigheten har. Befogenheterna i *första* och *tredje styckena* är oförändrade.

I det ändrade *andra stycket* har ett förtydligande tillägg gjorts, eftersom lagen nu omfattar tillsyn även över den europeiska digitala identitetsplånboken dess tillhandahållare. Den reviderade eIDAS-förordningen medger inte att förelägganden och förbud förenas med vite såvitt avser dessa tillsynsobjekt.

Övervägandena finns i avsnitt 6.6.1.

Administrativa sanktionsavgifter för betrodda tjänster

20 §

Tillsynsmyndigheten får besluta om sanktionsavgifter enligt EU:s förordning om elektronisk identifiering i dess lydelse enligt Europaparlamentets och rådets förordning (EU) 2024/1183 av den 11 april 2024 om ändring av förordning (EU) nr 910/2014 vad gäller inrättandet av ett europeiskt ramverk för digital identitet. Sådana sanktionsavgifter får tas ut av kvalificerade och icke-kvalificerade tillhandahållare av betrodda tjänster som:

- 1. utger sig för att vara en kvalificerad tillhandahållare utan att vara det eller tillhandahåller en icke-kvalificerad betrodd tjänst som utges vara kvalificerad,*
- 2. har lämnat oriktiga eller ofullständiga uppgifter vid ansökan om att bli kvalificerad,*
- 3. innehar status som kvalificerad tillhandahållare av betrodda tjänster eller har en kvalificerad betrodd tjänst, och inte i enlighet med artikel 24.2 a i nämnda förordning informerar om ändring av tillhandahållandet av tjänsten eller en avsikt att upphöra med verksamheten,*
- 4. missbrukar EU-förtroendemärket för kvalificerade betrodda tjänster,*
- 5. underlåter att rapportera om sådana incidenter som ska rapporteras enligt artikel 19a.1 b och artikel 24.2 fb i nämnda förordning, eller*
- 6. överträder ett beslut av tillsynsmyndigheten om föreläggande som innebär ett förbud.*

I paragrafen, som är ny, finns reglering om de överträdelser av regelverket, såvitt avser betrodda tjänster, som kan föranleda att en sanktionsavgift får tas ut av den som har gjort sig skyldig till överträdelsen. Det är alltså inte obligatoriskt för tillsynsmyndigheten att besluta om sanktionsavgift.

Strikt ansvar för överträdelser gäller. Det innebär att det inte krävs att det föreligger någon form av uppsåt eller oaktsamhet hos den som gjort sig skyldig till överträdelsen, utan det är tillräckligt att en överträdelse ägt rum. Av 22 och 23 §§ framgår att tillsynsmyndigheten ska beakta olika omständigheter vid prövningen av avgiftens storlek.

Enligt *punkten 1* kan tillsynsmyndigheten besluta om en sanktionsavgift om en tillhandahållare utger sig för att vara en kvalificerad tillhandahållare utan att vara det eller om den betrodda tjänst som utges vara kvalificerad inte är det.

Av *punkten 2* följer att en sanktionsavgift kan tas ut om en tillhandahållare har lämnat oriktiga eller ofullständiga uppgifter vid ansökan om att bli kvalificerad. För att sanktionsavgiften ska tas ut ska det röra sig om uppgifter av betydelse. Uppgifter av betydelse kan exempelvis vara sådana som hade inverkat på tillsynsmyndighetens

bedömning vid ansökan eller som kan bedömas utgöra en säkerhetsbrist.

Av *punkten 3* följer att tillsynsmyndigheten kan besluta om en sanktionsavgift om tillhandahållare som innehar status som kvalificerad tillhandahållare av betrodda tjänster eller har en kvalificerad betrodd tjänst, och inte i enlighet med artikel 24.2 a i den reviderade eIDAS-förordningen informerar om någon ändring av tillhandahållandet av tjänsten eller en avsikt att upphöra med verksamheten. För att sanktionsavgift ska tas ut ska det röra sig om omfattande förändringar, sårbarheter eller oriktigheter som upptäcks och som hade påverkat överensstämelsen med de säkerhetskrav som gäller för den kvalificerade tillhandahållaren och tjänsten.

Enligt *punkten 4* kan sanktionsavgift tas ut av tillhandahållare som missbrukar EU-förtroendemärket på så sätt att märket används för kvalificerade betrodda tjänster av tillhandahållare som inte är kvalificerad eller för betrodda tjänster som inte är kvalificerade.

Av *punkten 5* följer att tillsynsmyndigheten kan besluta om sanktionsavgift om en tillhandahållare underlåter att rapportera om sådana incidenter som ska rapporteras enligt artikel 19a och artikel 24.2 fb i den reviderade eIDAS-förordningen.

Enligt *punkten 6* kan tillhandahållare som överträder ett beslut av tillsynsmyndigheten om föreläggande som innebär ett förbud kan påföras sanktionsavgift. Utdömmande av sanktionsavgift enligt denna punkt hindras dock av bestämmelsen i 24 §.

Övervägandena finns i avsnitten 6.6.7, 6.6.8 och 6.6.10.

21§

En sanktionsavgift ska för fysiska personer bestämmas till lägst 5 000 kronor och högst ett belopp motsvarande 5 miljoner euro.

En sanktionsavgift för juridiska personer ska bestämmas till lägst 5 000 kronor och högst det högsta av ett belopp motsvarande 5 miljoner euro respektive en procent av den totala globala årsomsättningen för det företag som tillhandahållaren av betrodda tjänster tillhörde under det räkenskapsår som föregick det år då överträdelsen inträffade.

I paragrafen, som är ny, regleras sanktionsavgifternas storlek. Hur avgiften ska bestämmas i det enskilda fallet regleras i 22 §. Det är tillsynsmyndigheten som beslutar om sanktionsavgiftens storlek.

Enligt *första stycket* ska sanktionsavgift för fysiska personer bestämmas till lägst 5 000 kronor och högst ett belopp motsvarande 5 miljoner euro.

Enligt *andra stycket* ska sanktionsavgift för juridiska personer bestämmas till lägst 5 000 kronor och högst det högsta av ett belopp motsvarande 5 miljoner euro respektive en procent av den totala globala årsomsättningen för det företag som tillhandahållaren av betrodda tjänster tillhörde under det räkenskapsår som föregick det år då överträdelsen inträffade.

Övervägandena finns i avsnitt 6.6.11.

22 §

När sanktionsavgiftens storlek bestäms ska särskild hänsyn tas till berörd enhets storlek, affärsmodeller och överträdelsernas allvar.

Paragrafen är ny och reglerar vilka omständigheter som särskilt ska beaktas när tillsynsmyndigheten bestämmer sanktionsavgiftens storlek.

Vid bestämmande av storleken på sanktionsavgiften i det enskilda fallet bör hänsyn tas till alla relevanta omständigheter, särskilt den skada eller risk för skada som uppstått till följd av överträdelsen, om aktören tidigare begått en överträdelse och de kostnader som aktören undvikit till följd av regelöverträdelsen.

Skäl för att jämka en sanktionsavgift framgår av 23 §.

Övervägandena finns i avsnitt 6.6.11.

23 §

Tillsynsmyndigheten ska få sätta ner sanktionsavgiften helt eller delvis om överträdelsen är ringa eller ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften.

I paragrafen, som är ny, regleras jämkning av sanktionsavgift.

Av paragrafen följer att tillsynsmyndigheten kan sätta ned sanktionsavgiften, helt eller delvis, om överträdelsen är ringa, om det finns särskilda skäl eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften.

Det kan exempelvis vara oskäligt att ta ut en avgift om den avgiftsskyldige redan har drabbats av en sanktionsavgift enligt något annat

regelverk för i princip samma brist. Att regelverket har överträtts på ett sådant sätt att det varit närmast omöjligt för den avgiftsskyldige att upptäcka överträdelsen eller överträdelsen på annat sätt varit utom den avgiftsskyldiges kontroll, kan i undantagsfall göra överträdelsen ursäktlig och därför utgöra grund för jämkning.

Andra omständigheter att beakta i mildrande riktning kan vara att den avgiftsskyldige har samarbetat med tillsynsmyndigheten för att komma till rätta med överträdelsen eller skyndsamt har vidtagit rätelse för att minska skadan eller risken för skada.

Regleringen i 21 § om sanktionsavgifternas storlek hindrar inte ett beslut om jämkning som innebär att sanktionsavgift tas ut med ett belopp som är lägre än 5 000 kronor.

Möjligheten att sätta ner avgiften bör tillämpas restriktivt och endast när det skulle te sig oskäligt att ta ut avgiften.

Övervägandena finns i avsnitt 6.6.11.

24 §

En sanktionsavgift får inte beslutas om överträdelsen omfattas av ett föreläggande om vite och överträdelsen ligger till grund för en ansökan om utdömande av vitet.

Paragrafen är ny och innehåller ett förbud mot beslut om sanktionsavgifter i angivet fall. Paragrafen syftar till att förhindra att samma överträdelse blir föremål för dubbla prövningar och sanktioner.

Om ett beslut om vitesföreläggande har meddelats och en domstolsprocess inletts om utdömande av vitet är tillsynsmyndigheten enligt bestämmelsen förhindrad att besluta om sanktionsavgift för samma överträdelse. Bestämmelsen hindrar inte att en överträdelse först kan bli föremål för ett vitesföreläggande och i ett senare skede beslut om sanktionsavgift, under förutsättning att någon ansökan om utdömande av vitet inte har gjorts.

Övervägandena finns i avsnitt 6.6.12.

25 §

En sanktionsavgift får endast beslutas om den som avgiften ska tas ut av har fått tillfälle att yttra sig inom två år från det att överträdelsen ägde rum.

Ett beslut om sanktionsavgift ska delges.

I paragrafen, som är ny, regleras när en sanktionsavgift får beslutas och krav på delgivning.

Första stycket innebär att om kommunikation enligt förvaltningslagen med den som avgiften ska tas ut av inte har gjorts inom två år från den dag då överträdelsen ägde rum, får en sanktionsavgift inte tas ut. Bevisbördan för att kommunikation har genomförts ligger på tillsynsmyndigheten.

Av andra stycket framgår att ett beslut om sanktionsavgift ska delges. Det innebär att myndigheten ska använda sig av de metoder för delgivning som regleras i delgivningslagen.

Övervägandena finns i avsnitt 6.6.9.

26 §

Sanktionsavgiften tillfaller staten.

Paragrafen är ny och anger att en sanktionsavgift tillfaller staten.

Övervägandena finns i avsnitt 6.6.9.

27

En sanktionsavgift ska betalas till tillsynsmyndigheten inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet.

Om sanktionsavgiften inte betalas inom föreskriven tid, ska myndigheten lämna den obetalda avgiften för indrivning.

Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m. Vid indrivning får verkställighet ske enligt utsökningsbalken.

Paragrafen är ny och reglerar betalning och indrivning av sanktionsavgifter.

Övervägandena finns i avsnitt 6.6.9.

28 §

En beslutad sanktionsavgift faller bort till den del beslutet om avgiften inte har verkställts inom fem år från det att beslutet fick laga kraft.

Paragrafen, som är ny, reglerar preskription av sanktionsavgifter. Bestämmelsen innebär att betalning av beslutad avgift inte kan krävas efter det att fem år gått sedan beslutet fick laga kraft.

Övervägandena finns i avsnitt 6.6.9.

Avgifter

29 §

Regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten får meddela föreskrifter om skyldighet för tillhandahållare av betrodda tjänster och tillhandahållare av europeiska digitala identitetsplånböcker att betala avgift för tillsynsmyndighetens verksamhet enligt denna lag.

Paragrafen reglerar avgiftssystem för att finansiera tillsynsmyndighetens verksamhet enligt lagen. Tillägget i paragrafen tydliggör att även tillhandahållare av europeiska digitala identitetsplånböcker kan åläggas avgift för tillsynsverksamheten.

30 §

Regeringen eller, efter regeringens bemyndigande, de myndigheter som avses i 6 § första stycket och 9 § får meddela föreskrifter om skyldighet för juridiska personer att betala avgift för att tillhandahållas en europeisk digital identitetsplånbok respektive uppgifter för personidentifiering enligt denna lag och föreskrifter som meddelats med stöd av den.

Paragrafen, som är ny, reglerar möjlighet att införa ett avgiftssystem för att till juridiska personer tillhandahålla den europeiska digitala identitetsplånboken och uppgifter för personidentifiering (LPID). Det följer direkt av den reviderade eIDAS-förordningen att tillhandahållande, användning och återkallelse av sådana identitetsplånböcker, inbegripet uppgifter för personidentifiering (PID) ska ske utan kostnad för fysiska personer (artikel 5a.13).

Övervägandena finns i avsnitten 6.3.1 och 6.3.3.

Överklagande

31 §

Beslut av den myndighet som tillhandahåller uppgifter för personidentifiering liksom den tillhandahållande myndighetens och tillsynsmyndighetens beslut enligt EU:s förordning om elektronisk identifiering och rättsakter som har meddelats med stöd av den förordningen, samt enligt denna lag och föreskrifter som har meddelats med stöd av lagen får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Av paragrafen framgår att beslut ska överklagas till allmän förvaltningsdomstol. Endast den som beslutet angår får överklaga det och endast om det har gått honom eller henne emot (42 § förvaltningslagen).

Tilläggen i *första stycket* tydliggör att rätten till överklagande omfattar även beslut som fattas av den myndighet som tillhandahåller den europeiska digitala identitetsplån boken samt den eller de myndigheter som tillhandahåller uppgifter för personidentifiering (PID och LPID).

Övervägandena finns i avsnitt 6.7.

Ikraftträdande- och övergångsbestämmelser

- 1. Denna lag träder i kraft den 1 oktober 2025.*
- 2. Äldre bestämmelser gäller för överträdelser som ägt rum före ikraftträdandet.*

Punkten 1 anger när lagen träder i kraft. Regleringen i *punkten 2* innebär att nuvarande bestämmelser fortfarande ska gälla för överträdelser som har ägt rum före ikraftträdandet.

Övervägandena finns i kapitel 7.

9.2 Förslaget till förordning om ändring i förordningen (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering

Elektronisk identifiering

2 §

Anslutningsskyldigheten i 2 § lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering gäller inte för Säkerhetspolisen eller myndigheter som hör till Försvarsdepartementet.

Övervägandena finns i avsnitt 6.2.

4 §

Myndigheten för digital förvaltning ska till noden för inkommande gränsöverskridande elektronisk identifiering på begäran ansluta dem som uppfyller kraven för en sådan anslutning trots att de inte omfattas av anslutningsskyldigheten i 2 § lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

Myndigheten får ta ut avgifter av de privata aktörer som har anslutit sig till noden för inkommande gränsöverskridande elektronisk identifiering som myndigheten tillhandahåller.

Övervägandena finns i avsnitt 6.2.

Europeisk digital identitetsplånbok

7 §

Myndigheten för digital förvaltning ska vara den tillhandahållande myndigheten enligt 6 § första stycket lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering såvitt avser tillhandahållandet av en europeisk digital identitetsplånbok för både fysiska och juridiska personer.

Övervägandena finns i avsnitt 6.3.1.

8 §

Myndigheten för digital förvaltning ska meddela föreskrifter om villkor för godkännande som tillhandahållare av en europeisk digital identitetsplånbok och hur granskningsförfarandet enligt 6 § andra stycket lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering ska gå till,

Myndigheten får meddela föreskrifter om

1. sådana undantag från kravet att tillhandahålla öppen källkod som avses i artikel 5a.3 i EU:s förordning om elektronisk identifiering, och

2. sådana ytterligare funktioner för den europeiska digitala identitetsplånboken som avses i artikel 5a.7 i EU:s förordning om elektronisk identifiering.

Övervägandena finns i avsnitten 6.3.1 och 6.3.2.

9 §

Myndigheten för digital förvaltning ska i fråga om fysiska personer tillhandahålla sådana uppgifter för personidentifiering som avses i artikel 3 i EU:s förordning om elektronisk identifiering, och som ska kunna kopplas till den europeiska digitala identitetsplånboken.

Bolagsverket ska i fråga om juridiska personer tillhandahålla sådana uppgifter för personidentifiering som avses i artikel 3 i EU:s förordning om elektronisk identifiering, och som ska kunna kopplas till den europeiska digitala identitetsplånboken.

Myndigheterna får ta ut avgift av en juridisk person som tillhandahålls en europeisk digital identitetsplånbok och uppgifter för personidentifiering.

Övervägandena finns i avsnitten 6.3.1 och 6.3.3.

10 §

Myndigheten för digital förvaltning ska tillhandahålla en sådan valideringsmekanism som avses i 10 § 1 lagen (2016:561) om elektronisk identifiering.

Post- och telestyrelsen ska tillhandahålla sådana en sådan valideringsmekanism som avses i 10 § 2 lagen (2026:561) om elektronisk identifiering.

Övervägandena finns i avsnitt 6.3.5.

11 §

Den databas som Myndigheten för digital förvaltning ska föra enligt 11 § lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering ska i fråga om en fysisk person innehålla

1. fullständigt namn, personnummer alternativt samordningsnummer för personer med styrkt identitet, och födelsetid för användaren av den tillhandahållna europeiska digitala identitetsplånboken,

2. uppgift om det medel för elektronisk identifiering med vilket användaren har styrkt sin identitet,

3. uppgift som på ett unikt sätt identifierar den tillhandahållna europeiska digitala identitetsplånboken, och

4. uppgift om status för en tillhandahållen europeisk digital identitetsplånbok, om den har återkallats samt skälen för det.

Utöver det som anges i första stycket 3–4 ska databasen, i fråga om en juridisk person, innehålla uppgifter om dess namn och organisationsnummer.

Övervägandena finns i avsnitt 6.3.9.

12 §

Databasen som avses i 11 § får tillföras sådana uppgifter från Skatteverkets folkbokförings-databas som anges i 11 § första stycket 1.

Övervägandena finns i avsnitt 6.3.9.

13 §

Uppgifter och handlingar vilka finns i databasen som avses i 11 § ska gallras senast tio år efter utgången av det kalenderår då

1. den europeiska digitala identitetsplånboken tillhandahölls, eller

2. ett ärende om återkallelse avslutades.

Myndigheten för digital förvaltning får meddela närmare föreskrifter om integritetshöjande åtgärder till skydd för personuppgifter i databasen.

Övervägandena finns i avsnitt 6.3.9.

Certifiering

14 §

Försvarets materielverk ska utse ansvarigt organ för sådan certifiering av den europeiska digitala identitetsplån boken och system för elektronisk identifiering som avses i artikel 5c.1 i EU:s förordning om elektronisk identifiering samt sådan certifiering av anordningar för skapande av kvalificerade elektroniska underskrifter och anordningar för skapande av kvalificerade elektroniska stämplor som avses i artikel 30 och 39 i nämnd förordning.

Övervägandena finns i avsnitten 6.3.7 och 6.5.3.

Ikraftträdande

Denna förordning träder i kraft den 1 oktober 2025.

Övervägandena finns i kapitel 7.

9.3 Förslaget till förordning om ändring i förordningen (2007:951) med instruktion för Post- och telestyrelsen

4 §

Post- och telestyrelsen har till uppgift att

1. främja tillgången till säkra och effektiva elektroniska kommunikationer, inbegripet att se till att samhällsomfattande tjänster finns tillgängliga, och att främja tillgången till ett brett urval av elektroniska kommunikationstjänster,

2. främja utbyggnaden av och följa tillgången till bredband och mobil-täckning i alla delar av landet, inbegripet att skapa förutsättningar för samverkan mellan myndigheter som kan bidra till utbyggnaden av bredband,

3. svara för att möjligheterna till radiokommunikation och andra användningar av radiovågor utnyttjas effektivt,

4. svara för att nummer ur nationella nummerplaner utnyttjas på ett effektivt sätt,

5. främja en effektiv konkurrens,

6. övervaka pris- och tjänsteutvecklingen,

7. bedriva informationsverksamhet riktad till konsumenter,

8. följa utvecklingen när det gäller säkerhet vid elektronisk kommunikation och uppkomsten av eventuella miljö- och hälsorisker,

9. pröva frågor om tillstånd och skyldigheter, fastställa och analysera marknader samt utöva tillsyn och pröva tvister enligt lagen (2022:482) om elektronisk kommunikation,

10. meddela föreskrifter enligt förordningen (2022:511) om elektronisk kommunikation,

11. upprätta och offentliggöra planer för frekvensfördelning till ledning för radioanvändningen samt offentliggöra information av allmänt intresse om rättigheter, villkor, förfaranden och avgifter som rör radiospektrum-användningen,

12. tillhandahålla information om frekvensanvändning till Europeiska radiokommunikationskontorets frekvensinformationssystem (EFIS),

13. vara marknadskontrollmyndighet enligt radioutrustningslagen (2016:392),

14. vara tillsynsmyndighet enligt lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering *och utgöra gemensam kontaktpunkt för betrodda tjänster, europeiska digitala identitets-plånböcker och anmälda system för elektronisk identifiering enligt Europaparlamentets och rådets förordning (EU) 2024/1183 av den 11 april 2024 om ändring av förordning (EU) nr 910/2014 vad gäller inrättandet av ett europeiskt ramverk för digital identitet* samt ge stöd och information till myndigheter och enskilda när det gäller betrodda tjänster,

15. följa utvecklingen när det gäller toppdomäner med geografiska namn som har anknytning till Sverige,

16. vara tillsynsmyndighet enligt lagen (2006:24) om nationella toppdomäner för Sverige på internet samt meddela föreskrifter enligt förordningen (2006:25) om nationella toppdomäner för Sverige på internet,

17. verka för robusta elektroniska kommunikationer och minska risken för störningar, inbegripet att upphandla förstärkningsåtgärder, och verka för ökad krishanteringsförmåga,

18. verka för ökad nät- och informationssäkerhet i fråga om elektronisk kommunikation, genom samverkan med myndigheter som har särskilda uppgifter inom informationssäkerhets-, säkerhetsskydds- och integritetsskyddsområdet samt med andra berörda aktörer,

19. lämna råd och stöd till myndigheter, kommuner och regioner och till företag, organisationer och andra enskilda i frågor om nätsäkerhet,

20. vara tvistlösnings- och tillsynsmyndighet enligt lagen (2016:534) om åtgärder för utbyggnad av bredbandsnät och ansvara för informationstjänsten för utbyggnad av bredbandsnät enligt samma lag, och

21. vara tillsynsmyndighet enligt lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Övervägandena finns i avsnitten 6.2 och 6.6.2.

Ikraftträdande

Denna förordning träder i kraft den 1 oktober 2025.

Övervägandena finns i kapitel 7.

9.4 Förslaget till förordning om ändring i förordningen (2007:1110) med instruktion för Bolagsverket

2 b §

Bolagsverket ska i fråga om juridiska personer ansvara för tillhandahållandet av sådana personidentifieringsuppgifter som ska kunna kopplas till den europeiska digitala identitetsplånboken i enlighet med Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (EU:s förordning om elektronisk identifiering).

Övervägandena finns i avsnitten 6.3.3.

Ikraftträdande

Denna förordning träder i kraft den 1 oktober 2025.

Övervägandena finns i kapitel 7.

9.5 Förslaget till ändring i offentlighets- och sekretessförordningen (2009:641)

6 §

Sekretess gäller i nedan angiven verksamhet, som avser registrering av betydande del av befolkningen, för

1. uppgift om en enskilds personliga förhållanden, om det av särskild anledning kan antas att den enskilde eller någon närstående till honom eller henne lider men om uppgiften röjs, och

2. uppgift i form av fotografisk bild av den enskilde, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider men.

För uppgift i en allmän handling gäller sekretessen i högst sjuttio år.

Verksamheten avser

fastighetsregistret

kommunala fastighetsregister

Myndigheten för digital förvaltnings databas över den europeiska digitala identitetsplånboken

passregister och register över

nationella identitetskort
röstlängdsregister
Skatteverkets databas över
identitetskort för folkbokförda i Sverige
Socialstyrelsens register över
legitimerad hälso- och sjukvårdspersonal och personal med bevis om rätt
att använda yrkestiteln undersköterska
Statens jordbruksverks register över hund- och kattägare
Statens tjänstepensionsverks pensionsregister
Totalförsvarets plikt- och prövningsverks register över totalförsvarets per-
sonal
Transportstyrelsens vägtrafikregister

Övervägandena finns i avsnitt 6.3.10.

Ikraftträdande

Denna förordning träder i kraft den 1 oktober 2025.

Övervägandena finns i kapitel 7.

9.6 Förslaget till förordning om ändring i förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning

3 §

Myndigheten ska

1. ansvara för den offentliga förvaltningens tillgång till infrastruktur och tjänster för elektronisk identifiering och underskrift,

2. främja användningen av elektronisk identifiering och underskrift,

3. ansvara för de svenska förbindelsepunkterna (noderna) för gränsöverskridande elektronisk identifiering i enlighet med Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (eIDAS-förordningen) samt rättsakter som har meddelats med stöd av förordningen, och

4. *ansvara för tillhandahållandet av en europeisk digital identitetsplånbok i enlighet med eIDAS-förordningen samt, i fråga om fysiska personer, även tillhandahålla sådana uppgifter för personidentifiering som avses i artikel 3 i eIDAS-förordningen vilka ska kunna kopplas till den europeiska digitala identitetsplånboken.*

Övervägandena finns i avsnitt 6.3.1 och 6.3.3.

Ikraftträdande

Denna förordning träder i kraft den 1 oktober 2025.

Övervägandena finns i kapitel 7.

Kommittédirektiv 2022:142

Säker och tillgänglig digital identitet

Beslut vid regeringssammanträde den 22 december 2022

Sammanfattning

En särskild utredare ska utreda och lämna förslag på hur staten kan utfärda en e-legitimation på högsta tillitsnivå. Utredaren ska också se över behovet av Anpassningar som följer av den reviderade eIDAS-förordningen. Syftet är att stärka samhällets säkerhet och robusthet, motverka bedrägerier som begås med hjälp av e-legitimationer och underlätta för så många som möjligt att kunna få tillgång till en e-legitimation.

Utredaren ska bl.a.

- lämna förslag på hur en kostnadseffektiv statlig e-legitimation på högsta tillitsnivå kan utformas och tillhandahållas av en statlig myndighet,
- analysera och föreslå förändringar som följer av den reviderade eIDAS-förordningen, och
- lämna nödvändiga författningsförslag.

Uppdraget att föreslå hur staten kan utfärda en e-legitimation på högsta tillitsnivå ska delredovisas senast den 16 oktober 2023. Uppdraget ska slutredovisas senast den 31 maj 2024.

Säker och tillgänglig identifiering i ett digitaliserat samhälle

Den 3 juni 2021 presenterade Europeiska kommissionen ett förslag till Europaparlamentets och rådets förordning om ändring av förordning (EU) nr 910/2014 vad gäller inrättandet av en ram för europeisk digital identitet (den reviderade eIDAS-förordningen), COM(2021) 281. Det föreslås bl.a. att det ska bli obligatoriskt för varje medlemsstat att anmäla en e-legitimation på den högsta tillitsnivån enligt ett förfarande för gränsöverskridande identifiering och att varje medlemsstat ska utfärda en europeisk digital identitetsplånbok. Tillitsnivån på e-legitimationen avgör hur tillförlitligt det är att personen som identifierar sig är den man utger sig för att vara. Plånboken ska möjliggöra för fysiska och juridiska personer att på ett säkert sätt bl.a. begära, erhålla, lagra och använda personidentifieringsuppgifter och digitala bevis för autentisering online och offline samt att skriva under med kvalificerade elektroniska underskrifter.

Den ökade digitaliseringen gör det allt svårare att klara sig i samhället utan tillgång till en e-legitimation. Det är därför viktigt att så många som möjligt ges möjlighet att skaffa en säker e-legitimation. En e-legitimation är i princip nödvändig för att få tillgång till viktiga digitala tjänster och samhällsfunktioner, t.ex. hantera bankärenden eller för att ha kontakt med det offentliga. E-legitimationer har också börjat användas för identifiering exempelvis via telefon eller vid besök. En e-legitimation är alltså viktig för att enskilda ska kunna nyttja samhällets digitala tjänster så att alla enskilda kan ta till vara sina intressen och medborgerliga rättigheter. Detta gäller även för personer som bara tillfälligt vistas i Sverige, exempelvis för arbete.

I dag är det endast privata aktörer som utfärdar e-legitimationer och staten har begränsade möjligheter till insyn och påverkan. Det finns även behov av att utreda alternativa lösningar för e-legitimation utifrån flera perspektiv, särskilt när det gäller säkerhet, redundans och tillgänglighet.

E-legitimationer utgör en samhällsviktig infrastruktur som behöver fungera också om samhället utsätts för en stor påfrestning och ytterst även i krig. Störningar i e-legitimationssystem kan snabbt få kännbara effekter för näringsliv, banker, offentlig sektor och inte minst för enskilda även under i övrigt normala förhållanden.

Uppdraget att föreslå hur staten kan utfärda en e-legitimation på högsta tillitsnivå

Förslagen i revisionen av eIDAS-förordningen ställer krav på medlems-staterna att anmäla en e-legitimation på högsta tillitsnivå enligt ett särskilt anmälningsförfarande. En anmäld e-legitimation kan där- efter användas i andra EU-länders e-tjänster.

Det är viktigt i ett digitalt samhälle att så många som möjligt ges möjlighet att identifiera sig. En säker elektronisk identifiering kan också bidra till att motverka den identitetsrelaterade brottsligheten. Med en säker grundidentifiering som görs av en myndighet vid ett personligt besök minskar risken för att fel person får tillgång till e-legitimationen. En utredning ska analysera vilka kontroller av identiteten som behöver vidtas och om omfattningen av kontrollen ska vara jämförbar med den kontroll som sker för andra identitetshandlingar.

Utgångspunkten är att utfärdande av e-legitimationer på den högsta tillitsnivån bör ske vid en statlig myndighet. En e-legitimation på högsta nivå kan användas för växling till en annan e-legitimation på samma nivå eller en e-legitimation på lägre nivå.

För att en e-legitimation ska kunna användas behövs en bakomliggande digital infrastruktur mot vilken e-legitimationen kan verifieras. En individ kan använda sin e-legitimation flera gånger om dagen. Infrastrukturen behöver därför hantera en stor mängd verifieringar. Myndigheten för digital förvaltning ansvarar för den offentliga förvaltningens tillgång till infrastruktur och tjänster för elektronisk identifiering och underskrift. Eftersom system för e-legitimationer och digital identifiering kräver särskild kompetens bör Myndigheten för digital förvaltning vara den myndighet som får ett eventuellt uppdrag att ta fram en statlig e-legitimation.

2017 års ID-kortsutredning föreslår i sitt betänkande Ett säkert statligt ID-kort – med e-legitimation (SOU 2019:14) att staten ska utfärda en e-legitimation på högsta tillitsnivå. Syftet med förslaget är att ge alla invånare möjlighet att skaffa en säker e-legitimation för att de ska få tillgång till viktiga samhällsfunktioner. Vidare menar utredningen att en säker elektronisk identifiering motverkar den identitetsrelaterade brottsligheten.

Utredningen föreslår att en statlig e-legitimation ska finnas på det statliga identitetskort som enligt förslaget ska utfärdas av Polismyndigheten. Vidare konstaterar utredningen att det inte är möjligt att

uppskatta kostnaderna för bl.a. utveckling och förvaltning av e-legitimationen och lämnar inte heller förslag på en ersättningsmodell för utfärdande och användande av en e-legitimation. Utredningen konstaterade att det finns ett stort behov av alternativa lösningar för e-legitimationer.

Utredningens förslag bereds inom Regeringskansliet. Det är dock tidskrävande att ta fram ett kombinerat id-kort och e-legitimation. Förslagen i den reviderade eIDAS-förordningen i kombination med ett förändrat säkerhetsläge kan medföra vissa krav på skyndsamhet. Det kan därför finnas behov av en alternativ lösning för en e-legitimation på högsta nivå.

En ny utredning bör också analysera hur en e-legitimation kan utformas så att så många som möjligt kan få tillgång till den, exempelvis personer från andra länder som arbetar eller studerar i Sverige. Grupper som särskilt bör beaktas när förslagen utformas är bl.a. äldre och personer med funktionsnedsättning.

En statlig aktör som ansvarar för en e-legitimation kommer att behandla stora mängder personuppgifter om användarna. Det är därför viktigt att skyddet för den personliga integriteten beaktas, både utifrån bestämmelsen i 2 kap. 6 § andra stycket regeringsformen och Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

En del svenska medborgare bor utomlands och utredaren behöver analysera om de ska ha rätt att få tillgång till en e-legitimation från utlandet. Om utredaren bedömer att det bör finnas en sådan möjlighet, ska utredaren föreslå hur ansvarig myndighet kan tillhandahålla den.

Slutligen bör utredningen ta ställning till om en e-legitimation på högsta tillitsnivå ska kunna användas för att framställa kvalificerade elektroniska underskrifter. eIDAS-förordningen skiljer på avancerad elektronisk underskrift och kvalificerad elektronisk underskrift. På den senare ställs det högre säkerhetskrav. De underskrifter som finns på den svenska marknaden i dag är framför allt avancerade elektroniska underskrifter medan det i resten av Europa är mer vanligt med kvalificerade underskrifter.

Myndigheten för digital förvaltning fick våren 2022 ett uppdrag att i samarbete med Polismyndigheten och Försäkringskassan föreslå hur en statlig e-legitimation kan utformas (I2022/0135). Uppdraget

ska redovisas senast den 31 januari 2023. Utredningen ska i sitt arbete beakta förslagen och de synpunkter som framkommit inom ramen för regeringsuppdraget.

Utredaren ska därför

- lämna förslag på hur en kostnadseffektiv e-legitimation på tillitsnivå hög enligt eIDAS-förordningen kan utformas och tillhandahållas av Myndigheten för digital förvaltning,
- lämna förslag på vilken eller vilka myndigheter som ska ansvara för grundidentifieringen vid utfärdandet av en statlig e-legitimation och vilka kontroller av identitet som ska genomföras vid en sådan grundidentifiering,
- analysera om det bör ställas krav på förlitande parter som tillhandahåller digitala tjänster inom offentlig sektor att acceptera alla e-legitimationsalternativ på marknaden förutsatt att de lever upp till den tillitsnivå som tjänsterna kräver,
- analysera om det för vissa grupper kan behövas särskilda lösningar för att de ska kunna identifiera sig digitalt,
- analysera och beräkna kostnader för att ta fram och förvalta en e-legitimation och lämna förslag på hur en ersättningsmodell kan utformas där bl.a. avgifter för att få tillgång till en e-legitimation ska övervägas,
- analysera om e-legitimationen ska kunna användas för att framställa kvalificerade elektroniska underskrifter, och
- lämna nödvändiga författningsförslag.

Uppdraget att analysera och föreslå förändringar som följer av revisionen av eIDAS-förordningen

Om de föreslagna ändringarna i eIDAS-förordningen träder i kraft, innebär det att en rad nya krav måste mötas. Sverige måste exempelvis inrätta ett bedömningsorgan som har till uppdrag att certifiera e-legitimationslösningar som uppnår tillitsnivåerna i förordningen. Vidare ska valideringsmekanismer som säkerställer den digitala plånbokens äkthet införas. Medlemsstaterna kan också komma att behöva utarbeta processer för rapportering vid eventuell förlust och even-

tuellt missbruk av digitala plånböcker samt för återkallandet av sådana plånböcker. Vidare krävs det att medlemsstaterna inrättar ett organ som ansvarar för register över förlitande parter, dvs. fysiska eller juridiska personer som förlitar sig på en elektronisk identifiering.

Enligt förslaget ska ett tillsynsorgan ansvara för frågor som berör tillhanda-hållare av kvalificerade och icke-kvalificerade betrodda tjänster. Organet ska undersöka om betrodda tjänsterna uppfyller kraven i eIDAS-förordningen och kraven i Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen och de krav som den pågående revideringen av det direktivet föranleder.

Medlemsstaterna behöver vidare inkludera en unik och bestående identifikation-beteckning i minimiuppsättningen av personidentifieringsuppgifter för att kunna identifiera personen när identifiering krävs enligt lag.

De digitala plånböckerna ska enligt förslaget säkerställa att personidentifieringsuppgifter på ett unikt och beständigt sätt representerar den fysiska eller juridiska person som de är förbundna med. Plånböckerna ska tillhandahålla en mekanism som säkerställer att förlitande parter kan autentisera användaren och ta emot attributintyg. Det ska vidare säkerhetsställas att inte fler attribut än vad som är nödvändigt för tjänsten delas.

Myndigheten för digital förvaltning har i rapporten Digital plånbok (I2021/02470) föreslagit att svenska plånböcker ska utfärdas av en statlig myndighet och att även privata aktörer ska ges möjlighet till det. Syftet är att säkerställa att alla användare inkluderas, att systemet blir robust och att tillvarata innovation på området.

Utredaren ska därför

- utreda hur det kan säkerställas att en kostnadseffektiv digital identitetsplånbok i enlighet med den reviderade eIDAS-förordningen ska utfärdas,
- utreda hur en sådan digital plånbok kan användas ändamålsenligt för största möjliga nationella effektivitet och nytta,
- ta ställning till vilken myndighet som bör utses till tillsynsorgan med ansvar för ett register över förlitande parter enligt kraven i den reviderade eIDAS-förordningen,

- analysera den slutgiltiga versionen av förordningen i sin helhet och ge förslag på hur Sverige kan uppfylla tillkommande krav,
- föreslå de författningsändringar och andra åtgärder som krävs för att den föreslagna myndigheten ska kunna vidta de åtgärder som åläggs den enligt förordningen, samt
- lämna de författningsförslag i övrigt som är nödvändiga eller annars bedöms lämpliga för att komplettera förordningen.

Konsekvensbeskrivningar

Utredaren ska bedöma de ekonomiska konsekvenserna för myndigheter, regioner och kommuner av förslagen. Om förslagen kan förväntas leda till kostnadsökningar för ovan nämnda aktörer, ska utredaren föreslå hur dessa ska finansieras. Utredaren ska särskilt bedöma vilka organisatoriska och ekonomiska konsekvenser förslagen får för de myndigheter som berörs av förslagen. Utredaren ska också ange konsekvenser för enskilda och för företag i form av kostnader och ökade administrativa bördor samt om förslagen får några konsekvenser ur ett jämställdhetsperspektiv. Utredaren ska särskilt redovisa förslagets konsekvenser för den personliga integriteten och under arbetets gång göra en integritetsanalys. Utredaren ska också analysera eventuella risker för informationssäkerheten och risker med identitetsrelaterad brottslighet och redovisa konsekvenser för brottsbekämpningen och det brottsförebyggande arbetet.

Konsekvenserna ska redovisas enligt 14–15 a §§ kommittéförordningen (1998:1474) samt 6 och 7 §§ förordningen (2007:1244) om konsekvens-utredning vid regelgivning.

Kontakter och redovisning av uppdraget

Utredaren ska hålla sig informerad om och beakta relevant arbete som bedrivs inom Regeringskansliet, utredningsväsendet och inom EU, exempelvis Europeiska kommissionens förslag till förordning och direktiv om digitalisering av rättsligt samarbete.

Under genomförandet av uppdraget ska utredaren ha en dialog med och inhämta upplysningar från Ekobrottsmyndigheten, Finansinspektionen, Försvarsmakten, Försäkringskassan, Integritetsskyddsmyn-

digheten, Migrationsverket, Myndigheten för digital förvaltning, Myndigheten för samhällsskydd och beredskap, Riksarkivet, Skatteverket, Säkerhetspolisen, Polismyndigheten, Post- och telestyrelsen, näringslivet samt, i den utsträckning som utredaren finner det behövt, andra organisationer och myndigheter.

Följande uppdrag ska redovisas senast den 16 oktober 2023:

- Uppdraget att föreslå hur staten kan utfärda en e-legitimation på högsta tillitsnivå.

Följande uppdrag ska redovisas senast den 31 maj 2024:

- Uppdraget att analysera och föreslå förändringar som följer av revisionen av eIDAS-förordningen.

(Infrastrukturdepartementet)



2024/1183

30.4.2024

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2024/1183

av den 11 april 2024

om ändring av förordning (EU) nr 910/2014 vad gäller inrättandet av ett europeiskt ramverk för digital identitet

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 114,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande ⁽¹⁾,med beaktande av Regionkommitténs yttrande ⁽²⁾,i enlighet med det ordinarie lagstiftningsförfarandet ⁽³⁾, och

av följande skäl:

- (1) I kommissionens meddelande av den 19 februari 2020, Att *forma EU:s digitala framtid*, tillkännages att Europaparlamentets och rådets förordning (EU) nr 910/2014 ⁽⁴⁾ ska revideras i syfte att förbättra dess effektivitet, utvidga dess förmåner till den privata sektorn och främja betrodda digitala identiteter för alla europeer.
- (2) I sina slutsatser av den 1–2 oktober 2020 uppmanade Europeiska rådet kommissionen att föreslå en utveckling av ett unionsomfattande ramverk för säker offentlig elektronisk identifiering, inklusive interoperabla elektroniska underskrifter, så att människor kan ha kontroll över sin identitet och sina uppgifter på nätet och få tillgång till offentliga, privata och gränsöverskridande digitala tjänster.
- (3) I policyprogrammet för det digitala decenniet, inrättat genom Europaparlamentets och rådets beslut (EU) 2022/2481 ⁽⁵⁾, fastställs syftena och de digitala målen för ett unionsramverk som, senast 2030, är avsett att leda till en omfattande utbyggnad av en betrodd, frivillig och användarkontrollerad digital identitet som erkänns i hela unionen och som innebär att varje användare kan kontrollera sina uppgifter vid onlineinteraktioner.
- (4) I den europeiska förklaringen om digitala rättigheter och principer för det digitala decenniet, som kungjordes av Europaparlamentet, rådet och kommissionen ⁽⁶⁾ (*förklaringen*), understryks allas rätt att ha tillgång till digitala tekniker, produkter och tjänster som är säkra och trygga och utformade på ett sätt som skyddar den personliga integriteten. Detta inbegriper att säkerställa att alla människor i unionen erbjuds en tillgänglig, säker och tillförlitlig digital identitet som ger tillgång till ett brett utbud av nättjänster och offlinetjänster och som är skyddad mot cybersäkerhetsrisker och it-brottslighet, däribland personuppgiftsincidenter och stöld eller manipulation av identiteten. I förklaringen anges även att alla har rätt till skydd av sina personuppgifter. Denna rätt innefattar kontrollen över hur uppgifterna används och vem som får ta del av dem.

⁽¹⁾ EUT C 105, 4.3.2022, s. 81.

⁽²⁾ EUT C 61, 4.2.2022, s. 42.

⁽³⁾ Europaparlamentets ständpunkt av den 29 februari 2024 (ännu inte offentliggjord i EUT) och rådets beslut av den 26 mars 2024.

⁽⁴⁾ Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (EUT L 257, 28.8.2014, s. 73).

⁽⁵⁾ Europaparlamentets och rådets beslut (EU) 2022/2481 av den 14 december 2022 om inrättande av policyprogrammet för det digitala decenniet 2030 (EUT L 323, 19.12.2022, s. 4).

⁽⁶⁾ EUT C 23, 23.1.2023, s. 1.

- (5) Unionsmedborgarna och invånare i unionen bör ha en rätt till en digital identitet som står under deras egen kontroll och som innebär att de kan utöva sina rättigheter i den digitala miljön och delta i den digitala ekonomin. För att nå detta syfte bör ett europeiskt ramverk för digital identitet inrättas som ger unionsmedborgare och invånare i unionen tillgång till offentliga och privata nättjänster och offlinetjänster i hela unionen.
- (6) Ett harmoniserat ramverk för digital identitet bör bidra till att skapa en digitalt mer integrerad union genom att minska de digitala hindren mellan medlemsstaterna och ge unionsmedborgarna och invånare i unionen möjlighet att dra nytta av digitaliseringsens fördelar och samtidigt öka öppenheten och skyddet av deras rättigheter.
- (7) En mer harmoniserad strategi för elektronisk identifiering bör minska de risker och kostnader som den nuvarande fragmenteringen har lett till på grund av användningen av olika nationella lösningar eller, i vissa medlemsstater, frånvaron av sådana lösningar för elektronisk identifiering. En sådan strategi bör stärka den inre marknaden genom att göra det möjligt för unionsmedborgare, invånare i unionen enligt definitionen i nationell rätt och företag att identifiera sig och att autentisera sin identitet online och offline på ett säkert, tillförlitligt, användarvänligt, enkelt, tillgängligt och harmoniserat sätt i hela unionen. Den europeiska digitala identitetsplanboken bör förse fysiska och juridiska personer i hela unionen med harmoniserade medel för elektronisk identifiering som möjliggör autentisering och utbyte av data som är kopplade till deras identitet. Alla bör ha möjlighet att komma åt offentliga och privata tjänster på ett säkert sätt genom ett förbättrat ekosystem för betrodda tjänster och med verifierade identitetsbevis och elektroniska attributsintyg, till exempel akademiska kvalifikationer, inbegripet universitetsexamen eller andra utbildnings- eller yrkeskvalifikationer. Det europeiska ramverket för digital identitet är avsett att åstadkomma en övergång från användningen av endast nationella lösningar för elektronisk identifiering till tillhandahållande av elektroniska attributsintyg som är giltiga och rättsligt erkända i hela unionen. Tillhandahållare av elektroniska attributsintyg bör omfattas av en tydlig och enhetlig uppsättning av regler, medan offentliga förvaltningar bör kunna förlita sig på elektroniska dokument i ett visst format.
- (8) Flera medlemsstater har infört och använder medel för elektronisk identifiering som godtas av tjänsteleverantörer i unionen. Dessutom gjordes investeringar i både nationella och gränsöverskridande lösningar på grundval av förordning (EU) nr 910/2014, inbegripet interoperabilitet i anmälda system för elektronisk identifiering enligt den förordningen. För att säkerställa komplementaritet och ett snabbt ibrukttagande av europeiska digitala identitetsplanböcker av nuvarande användare av anmälda medel för elektronisk identifiering och för att minimera konsekvenserna för befintliga tjänsteleverantörer, förväntas de europeiska digitala identitetsplanböckerna dra nytta av att bygga vidare på erfarenheterna av befintliga medel för elektronisk identifiering och av infrastrukturen för anmälda system för elektronisk identifiering på unionsnivå och nationell nivå.
- (9) Europaparlamentets och rådets förordning (EU) 2016/679⁽⁷⁾ och, i förekommande fall, Europaparlamentets och rådets direktiv 2002/58/EG⁽⁸⁾ är tillämpliga på all behandling av personuppgifter i enlighet med förordning (EU) nr 910/2014. Lösningarna inom det interoperabilitetsramverk som föreskrivs i den här förordningen är också förenliga med dessa regler. Unionsrätten om dataskydd innehåller dataskyddsprinciper, såsom uppgiftsminimering och principen om ändamålsbegränsning, och skyldigheter, såsom inbyggt dataskydd och dataskydd som standard.
- (10) För att förbättra unionsföretagens konkurrenskraft bör tillhandahållare av både nättjänster och offlinetjänster kunna förlita sig på lösningar för elektronisk identifiering som erkänns i hela unionen, oavsett vilken medlemsstat dessa lösningar tillhandahålls i, och därmed dra nytta av en harmoniserad unionsstrategi för tillförlitlighet, säkerhet och interoperabilitet. Både användare och tjänsteleverantörer bör kunna gynnas av att samma rättsliga värde ges till elektroniska attributsintyg i hela unionen. Ett harmoniserat ramverk för digital identitet är avsett att skapa ekonomiskt värde genom att underlätta tillgången till varor och tjänster, genom att avsevärt minska driftskostnaderna för elektroniska identifierings- och autentiseringsförfaranden, t.ex. vid anslutning av nya kunder, genom att minska risken för it-brottslighet, såsom identitetsstöld, datastöld och nätbedrägeri, och på så sätt främja effektivitetsvinster och en säker digital omställning bland unionens mikroföretag och små och medelstora företag.
- (7) Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1).
- (8) Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) (EGT L 201, 31.7.2002, s. 37).

- (11) Europeiska digitala identitetsplånböcker bör underlätta tillämpningen av engångsprincipen och på så sätt minska den administrativa bördan och stödja gränsoverskridande rörlighet för unionsmedborgare och invånare i unionen och företag i unionen samt främja utvecklingen av interoperabla e-förvaltningstjänster i hela unionen.
- (12) Förordning (EU) 2016/679, Europaparlamentets och rådets förordning (EU) 2018/1725⁽⁹⁾ och direktiv 2002/58/EG är tillämpliga på behandlingen av personuppgifter i samband med genomförandet av denna förordning. Därför bör specifika skyddsåtgärder fastställas i denna förordning för att förhindra att tillhandahållare av medel för elektronisk identifiering och elektroniska attributsintyg kombinerar personuppgifter som erhållits vid tillhandahållande av andra tjänster med personuppgifter som behandlas för att tillhandahålla de tjänster som omfattas av tillämpningsområdet för denna förordning. Personuppgifter som rör tillhandahållandet av de europeiska digitala identitetsplånböckerna bör hållas logiskt avskilda från andra data som innehas av tillhandahållaren av den europeiska digitala identitetsplånboken. Denna förordning bör inte hindra tillhandahållare av europeiska digitala identitetsplånböcker från att tillämpa ytterligare tekniska åtgärder som bidrar till skyddet av personuppgifter, såsom fysisk åtskillnad mellan personuppgifter som rör tillhandahållandet av europeiska digitala identitetsplånböcker och andra uppgifter som innehas av tillhandahållaren. Utan att det påverkar tillämpningen av förordning (EU) 2016/679 specificeras i denna förordning ytterligare tillämpningen av principerna om ändamålsbegränsning, uppgiftsminimering, inbyggt dataskydd och dataskydd som standard.
- (13) De europeiska digitala identitetsplånböckerna bör ha en funktion i form av en gemensam instrumentpanel som är inbäddad i dess utformning för att säkerställa att användarna har en högre grad av öppenhet, integritet och kontroll när det gäller deras data. Den funktionen bör ha ett enkelt, användarvänligt gränssnitt med en översikt över alla förlitande parter med vilka användaren delar data, inklusive attribut, och vilken typ av uppgifter som delas med varje förlitande part. Den bör göra det möjligt för användare att spåra alla transaktioner som utförs genom den europeiska digitala identitetsplånboken med åtminstone följande uppgifter: tidpunkt och datum för transaktionen, identifiering av motparten, begärda personuppgifter och delade uppgifter. Denna information bör lagras även om transaktionen inte fullföljs. Det bör inte vara möjligt att bestrida äktheten hos den information som ingår i transaktionshistoriken. En sådan funktion bör vara aktiv som utgångspunkt. Den bör göra det möjligt för användare att enkelt begära att en förlitande part omedelbart raderar personuppgifter enligt artikel 17 i förordning (EU) 2016/679 och att enkelt rapportera den förlitande parten till den behöriga nationella dataskyddsmyndigheten om en påstått olaglig eller misstänkt begäran om personuppgifter tagits emot, direkt via den europeiska digitala identitetsplånboken.
- (14) Medlemsstaterna bör integrera olika integritetsbevarande tekniker, såsom nollkunskapsbevis, i den europeiska digitala identitetsplånboken. Dessa kryptografiska metoder bör göra det möjligt för en förlitande part att validera om ett visst påstående baserat på personens identifieringsuppgifter och attributsintyg är sant, utan att några uppgifter med anknytning till detta påstående förmedlas, och därigenom bevara användarens integritet.
- (15) Denna förordning fastställer harmoniserade villkor för inrättandet av ett ramverk för europeiska digitala identitetsplånböcker som ska tillhandahållas av medlemsstaterna. Alla unionsmedborgare och invånare i unionen enligt definitionen i nationell rätt bör på ett säkert sätt kunna begära, välja, kombinera, lagra, radera, dela och visa identitetsuppgifter och begära att deras personuppgifter raderas på ett användarvänligt och bekvämt sätt under användarens egen kontroll, samtidigt som selektivt utlämnande av personuppgifter möjliggörs. Denna förordning återspeglar gemensamma europeiska värden och respekterar grundläggande rättigheter, rättsliga garantier och ansvarsskyldighet, och skyddar därmed demokratiska samhällen, unionsmedborgare och invånare i unionen. De tekniker som används för att uppnå dessa mål bör utformas för att uppnå högsta möjliga nivå av säkerhet, integritet, användarvänlighet, tillgänglighet, användbarhet och sömlös interoperabilitet. Medlemsstaterna bör säkerställa lika tillgång till elektronisk identifiering för alla sina medborgare och invånare. Medlemsstaterna bör inte, varken direkt eller indirekt, begränsa tillgången till offentliga eller privata tjänster för fysiska eller juridiska personer som väljer att inte använda en europeisk digital identitetsplånbok och bör göra lämpliga alternativa lösningar tillgängliga.

⁽⁹⁾ Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39).

- (16) Medlemsstaterna bör förlita sig på de möjligheter som denna förordning erbjuder för att på eget ansvar tillhandahålla europeiska digitala identitetsplånböcker för användning av fysiska och juridiska personer som är bosatta på deras territorium. För att ge medlemsstaterna flexibilitet och öka utnyttjandet den senaste tekniken bör denna förordning möjliggöra tillhandahållande av europeiska digitala identitetsplånböcker direkt av en medlemsstat, på uppdrag av en medlemsstat eller oberoende av en medlemsstat men med erkännande av den medlemsstaten.
- (17) För registreringsändamål bör förlitande parter tillhandahålla den information som krävs för att möjliggöra elektronisk identifiering och autentisering av dem gentemot europeiska digitala identitetsplånböcker. När förlitande parter deklarerar sin avsedda användning av den europeiska digitala identitetsplånboken bör de tillhandahålla information om de uppgifter som de eventuellt kommer att begära för att tillhandahålla sina tjänster och om skälet till begäran. Registreringen av förlitande parter underlättar medlemsstaternas kontroller av lagenligheten hos de förlitande parternas verksamhet i enlighet med unionsrätten. Registreringsskyldigheten enligt denna förordning bör inte påverka de skyldigheter som fastställs i annan unionsrätt eller nationell rätt, såsom den information som ska lämnas till de registrerade i enlighet med förordning (EU) 2016/679. Förlitande parter bör följa de garantier som erbjuds genom artiklarna 35 och 36 i den förordningen, särskilt genom att utföra konsekvensbedömningar avseende dataskydd och genom att samråda med de behöriga dataskyddsmyndigheterna innan de behandlar uppgifter, om konsekvensbedömningar avseende dataskydd visar att behandlingen skulle leda till en hög risk. Sådana garantier bör utgöra ett stöd för förlitande parters lagliga behandling av personuppgifter, i synnerhet avseende särskilda kategorier av uppgifter, såsom hälsouppgifter. Registreringen av förlitande parter syftar till att öka öppenheten i och förtroendet för användningen av europeiska digitala identitetsplånböcker. Registreringen bör vara kostnadseffektiv och stå i proportion till de relaterade riskerna för att säkerställa att den sprids bland tjänsteleverantörerna. I detta sammanhang bör registreringen innebära att automatiserade förfaranden används, inbegripet att medlemsstaterna förlitar sig på och använder befintliga register, och den bör inte innefatta något förfarande för förhandsgodkännande. Registreringsprocessen bör möjliggöra en rad olika användningsfall som kan skilja sig åt i fråga om driftsätt – antingen online eller offline – eller i fråga om kravet på autentisering av enheter för interaktion med den europeiska digitala identitetsplånboken. Registreringen bör uteslutande gälla förlitande parter som tillhandahåller tjänster genom digital interaktion.
- (18) Att skydda unionsmedborgare och invånare i unionen mot obehörig eller bedräglig användning av europeiska digitala identitetsplånböcker är av stor betydelse för att säkerställa förtroende för och en bred spridning av europeiska digitala identitetsplånböcker. Användarna bör förses med ett effektivt skydd mot sådant missbruk. I synnerhet när fakta som utgör grunden för bedräglig eller annan olaglig användning av en europeisk digital identitetsplånbok fastställs av en nationell rättslig myndighet i samband med ett annat förfarande, bör tillsynsorgan som ansvarar för utfärdare av europeiska digitala identitetsplånböcker efter anmälan vidta nödvändiga åtgärder för att säkerställa att registreringen av den förlitande parten och inkluderingen av förlitande parter i autentiseringsmekanismen återkallas eller tillfälligt upphävs till dess att den anmälande myndigheten bekräftar att de konstaterade oriktigheterna har åtgärdats.
- (19) Alla europeiska digitala identitetsplånböcker bör göra det möjligt för användarna att identifiera och autentisera sig på elektronisk väg online och offline över gränserna för att få tillgång till ett stort utbud av offentliga och privata tjänster. Utan att det påverkar medlemsstaternas behörigheter när det gäller identifieringen av deras medborgare och invånare kan europeiska digitala identitetsplånböcker även användas för att tillgodose de institutionella behoven vid offentliga förvaltningar, internationella organisationer samt EU:s institutioner, organ och byråer. I många sektorer är det viktigt med autentisering offline, bland annat i hälso- och sjukvårdssektorn, där tjänsterna ofta tillhandahålls vid direkta kontakter, och e-recept bör kunna autentiseras med hjälp av QR-koder eller liknande tekniker. För att säkerställa en hög tillitnivå vad gäller system för elektronisk identifiering bör de europeiska digitala identitetsplånböckerna utnyttja den potential som erbjuds via manipuleringsssäkra lösningar såsom säkerhetsdetaljer för att uppfylla säkerhetskraven i denna förordning. Europeiska digitala identitetsplånböcker bör även göra det möjligt för användarna att skapa och använda kvalificerade elektroniska underskrifter och stämplat som godtas i hela unionen. När fysiska personer väl har börjat använda en europeisk digital identitetsplånbok bör de, som utgångspunkt och kostnadsfritt, kunna använda den för att underteckna med kvalificerade elektroniska underskrifter utan att behöva genomgå några ytterligare administrativa förfaranden. Användare bör kunna underteckna eller stämpla egna förklaringar eller attribut. För att ge personer och företag i hela unionen fördelar i form av enkel hantering och sänkta kostnader, däribland genom att tillåta behörigheter att företräda och elektroniska fullmakter, bör medlemsstaterna tillhandahålla europeiska digitala identitetsplånböcker på grundval av gemensamma standarder och tekniska specifikationer för att säkerställa sömlös interoperabilitet och på adekvat sätt höja it-säkerhetsnivån, stärka motståndskraften mot cyberattacker och på så vis avsevärt minska de potentiella riskerna med den pågående digitaliseringen för unionsmedborgare, invånare i unionen och företag. Det är endast medlemsstaternas behöriga

- myndigheter som kan fastställa identiteter med en hög tillförlitlighetsnivå och därmed garantera att en person faktiskt är den person som han eller hon påstår sig vara. Därför måste tillhandahållandet av de europeiska digitala identitetsplånböckerna bygga på den juridiska identiteten för unionsmedborgare, invånare i unionen eller juridiska personer. Användning av den juridiska identiteten bör inte hindra användarna av de europeiska digitala identitetsplånböckerna från att få tillgång till tjänster under en pseudonym om det inte finns något rättsligt krav på juridisk identitet för autentisering. Tilliten till de europeiska digitala identitetsplånböckerna skulle förstärkas om utfärdande och förvaltande parter hade varit tvungna att genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa den högsta säkerhetsnivå som står i rimlig proportion till riskerna för fysiska personers rättigheter och friheter i enlighet med förordning (EU) 2016/679.
- (20) Användningen av en kvalificerad elektronisk underskrift bör vara kostnadsfri för alla fysiska personer för icke-yrkesmässiga ändamål. Det bör vara möjligt för medlemsstaterna att föreskriva åtgärder för att hindra att fysiska personer kostnadsfritt använder kvalificerade elektroniska underskrifter för yrkesmässiga ändamål och samtidigt säkerställa att alla sådana åtgärder står i proportion till identifierade risker och är motiverade.
- (21) Det är fördelaktigt att underlätta spridningen och användningen av europeiska digitala identitetsplånböcker genom att på ett smidigt sätt integrera dem i ekosystemet av offentliga och privata digitala tjänster som redan införts på nationell, lokal eller regional nivå. För att uppnå detta mål bör medlemsstaterna kunna föreskriva rättsliga och organisatoriska åtgärder för att öka flexibiliteten för tillhandahållare av europeiska digitala identitetsplånböcker och medge ytterligare funktioner i de europeiska digitala identitetsplånböckerna utöver vad som fastställs i denna förordning, bland annat genom ökad interoperabilitet med befintliga nationella medel för elektronisk identifiering. Sådana ytterligare funktioner bör inte på något sätt inverka negativt på tillhandahållandet av de europeiska digitala identitetsplånböckernas centrala funktioner som föreskrivs i denna förordning och inte heller främja befintliga nationella lösningar framför europeiska digitala identitetsplånböcker. Eftersom sådana ytterligare funktioner går utöver denna förordning omfattas de inte av de bestämmelser om gränsöverskridande användning av europeiska digitala identitetsplånböcker som fastställs i denna förordning.
- (22) Europeiska digitala identitetsplånböcker bör ha en funktion för att generera pseudonymer, som användarna väljer och hanterar, för autentisering vid åtkomst till nättjänster.
- (23) För att uppnå en hög nivå av säkerhet och tillförlitlighet innehåller denna förordning krav för de europeiska digitala identitetsplånböckerna. Plånböckernas efterlevnad med dessa krav bör intygas av akkrediterade organ för bedömning av överensstämmelse som utses av medlemsstaterna.
- (24) För att undvika skilda tillvägagångssätt och harmonisera genomförandet av de krav som fastställs i denna förordning bör kommissionen, med avseende på certifiering av europeiska digitala identitetsplånböcker, anta genomförandeakter i syfte att fastställa en förteckning över referensstandarder och, vid behov, specifikationer och förfaranden i syfte att formulera närmare tekniska specifikationer av dessa krav. I den mån intyg om överensstämmelse för de europeiska digitala identitetsplånböckerna med relevanta cybersäkerhetskrav inte omfattas av befintliga ordningar för cybersäkerhetscertifiering som avses i denna förordning, och när det gäller andra krav än cybersäkerhetskrav som är relevanta för europeiska digitala identitetsplånböcker, bör medlemsstaterna inrätta nationella certifieringssystem i enlighet med de harmoniserade krav som fastställs i och antas i enlighet med denna förordning. Medlemsstaterna bör överföra sina utkast till nationella certifieringssystem till den europeiska samarbetsgruppen för digital identitet, som bör kunna utfärda yttranden och rekommendationer.
- (25) Certifiering av överensstämmelse med de cybersäkerhetskrav som fastställs i denna förordning bör, i förekommande fall, bygga på de relevanta europeiska ordningar för cybersäkerhetscertifiering som inrättats i enlighet med Europaparlamentets och rådets förordning (EU) 2019/881⁽¹⁰⁾, som inrättat en frivillig europeisk ram för cybersäkerhetscertifiering av IKT-produkter, IKT-processer och IKT-tjänster.

⁽¹⁰⁾ Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten) (EUT L 151, 7.6.2019, s. 15).

- (26) För att kontinuerligt bedöma och minska säkerhetsrelaterade risker bör certifierade europeiska digitala identitetsplånböcker bli föremål för regelbundna sårbarhetsbedömningar som syftar till att upptäcka eventuella sårbarheter i den europeiska digitala identitetsplånbokens certifierade produkt-, process- och tjänsterelaterade komponenter.
- (27) Genom att skydda användare och företag mot cybersäkerhetsrisker bidrar de väsentliga cybersäkerhetskrav som fastställs i denna förordning också till att förbättra skyddet av personuppgifter och individers integritet. När det gäller både standardiseringen och certifieringen av cybersäkerhetsaspekter bör synergier övervägas genom samarbete mellan kommissionen, europeiska standardiseringsorganisationer, Europeiska unionens cybersäkerhetsbyrå (Enisa), Europeiska dataskyddsstyrelsen, som inrättats genom förordning (EU) 2016/679, och de nationella tillsynsmyndigheterna med ansvar för dataskydd.
- (28) Anslutning av unionsmedborgare och invånare i unionen till den europeiska digitala identitetsplånboken bör underlättas genom att man förlitar sig på medel för elektronisk identifiering som utfärdats med tillitsnivå hög. Medel för elektronisk identifiering som utfärdats med tillitsnivå väsentlig bör endast användas om harmoniserade tekniska specifikationer och förfaranden med hjälp av medel för elektronisk identifiering som utfärdats med tillitsnivå väsentlig i kombination med kompletterande medel för kontroll av identitet möjliggör uppfyllande av kraven i denna förordning vad gäller tillitsnivå hög. Sådana kompletterande medel bör vara tillförlitliga och lätta att använda och skulle kunna bygga på möjligheten att använda förfaranden för anslutning på distans, kvalificerade certifikat som stöds av kvalificerade elektroniska underskrifter, kvalificerade elektroniska attributsintyg eller en kombination av dessa. För att säkerställa tillräcklig spridning av de europeiska digitala identitetsplånböckerna bör harmoniserade tekniska specifikationer och förfaranden för anslutning av användare med hjälp av medel för elektronisk identifiering, inbegripet sådana som utfärdats med tillitsnivå väsentlig, fastställas i genomförandeakter.
- (29) Syftet med denna förordning är att förse användaren med en helt mobil, säker och användarvänlig europeisk digital identitetsplånbok. Som en övergångsåtgärd till dess att certifierade manipuleringsssäkra lösningar, såsom säkerhetskomponenter i användarnas enheter, finns tillgängliga bör de europeiska digitala identitetsplånböckerna kunna förlita sig på certifierade externa säkerhetskomponenter för skyddet av kryptografiskt material och andra känsliga uppgifter eller på anmälda medel för elektronisk identifiering med tillitsnivå hög för att påvisa överensstämmelse med de relevanta kraven i denna förordning vad gäller den europeiska digitala identitetsplånbokens tillitsnivå. Denna förordning bör inte påverka nationella villkor avseende utfärdande och användning av certifierade externa säkerhetskomponenter om denna övergångsåtgärd är beroende av dessa.
- (30) De europeiska digitala identitetsplånböckerna bör garantera högsta möjliga dataskydds- och säkerhetsnivå för elektronisk identifiering och autentisering som underlättar tillgången till offentliga och privata tjänster, oavsett om uppgifterna lagras lokalt eller genom molnbaserade lösningar, där vederbörlig hänsyn tas till de olika risknivåerna.
- (31) De europeiska digitala identitetsplånböckerna bör ha inbyggd säkerhet och innefatta avancerade säkerhetsfunktioner för att skydda mot identitetsstöld och annan datastöld, tillgänglighetsförlust och alla andra cyberhot. Säkerheten bör innefatta toppmoderna krypterings- och lagringsmetoder som är tillgängliga och dekrypterbara endast för användaren, och som förlitar sig på totalsträckskrypterad kommunikation med andra europeiska digitala identitetsplånböcker och förlitande parter. Dessutom bör de europeiska digitala identitetsplånböckerna kräva en säker, uttrycklig och aktiv bekräftelse av användaren för de operationer som utförs via de europeiska digitala identitetsplånböckerna.
- (32) Kostnadsfri användning av europeiska digitala identitetsplånböcker bör inte leda till behandling av data utöver data som är nödvändig för tillhandahållandet av tjänster relaterade till europeiska digitala identitetsplånböcker. Denna förordning bör inte tillåta behandling av personuppgifter som lagras i eller härrör från användningen av den europeiska digitala identitetsplånboken av tillhandahållaren av den europeiska digitala identitetsplånboken för andra ändamål än tillhandahållandet av tjänster relaterade till europeiska digitala identitetsplånböcker. För att säkerställa integritet bör tillhandahållare av europeiska digitala identitetsplånböcker säkerställa icke-observerbarhet genom att inte samla in uppgifter och inte ha insyn i de transaktioner som utförs av användarna av den europeiska digitala identitetsplånboken. Denna icke-observerbarhet innebär att tillhandahållarna inte kan se detaljerade uppgifter om användarens transaktioner. I specifika fall, baserat på användarens uttryckliga föregående samtycke i vart och ett av dessa specifika fall, och i full överensstämmelse med förordning (EU) 2016/679, skulle tillhandahållare av europeiska

digitala identitetsplånböcker emellertid kunna beviljas tillgång till den information som krävs för tillhandahållandet av en viss tjänst som gäller europeiska digitala identitetsplånböcker.

- (33) Transparensen i europeiska digitala identitetsplånböcker och tillhandahållarnas ansvarsskyldighet är viktiga faktorer för att skapa social tillit och få till stånd acceptans för ramverket. De europeiska digitala identitetsplånböckernas funktions sätt bör därför vara transparent och i synnerhet medge kontrollerbar behandling av personuppgifter. För att uppnå detta bör medlemsstaterna lämna ut källkoden för programvarukomponenter i användartillämpningen av europeiska digitala identitetsplånböcker, inbegripet dem som rör behandling av personuppgifter och uppgifter om juridiska personer. Offentliggörandet av denna källkod under en licens med öppen källkod bör göra det möjligt för samhället, inbegripet användare och utvecklare, att förstå hur koden fungerar samt revidera och granska koden. Detta skulle öka användarnas förtroende för ekosystemet och bidra till de europeiska digitala identitetsplånböckernas säkerhet genom att göra det möjligt för vem som helst att rapportera sårbarheter och fel i koden. På det hela taget bör detta ge leverantörerna incitament att leverera och upprätthålla en mycket säker produkt. I vissa fall kan dock offentliggörandet av källkoden för bibliotek, kommunikationskanaler eller andra element som inte finns på användarenheten begränsas av medlemsstaterna, av vederbörligen motiverade skäl, särskilt med hänsyn till den allmänna säkerheten.
- (34) Att använda europeiska digitala identitetsplånböcker liksom att upphöra att använda dem bör vara användarens exklusiva rättighet och val. Medlemsstaterna bör utarbeta enkla och säkra förfaranden så att användarna kan begära att giltigheten för europeiska digitala identitetsplånböcker omedelbart återkallas, även i händelse av förlust eller stöld. Vid användarens död eller när en juridisk persons verksamhet upphör bör en mekanism inrättas som gör det möjligt för den myndighet som ansvarar för att reglera arvet efter den fysiska personen eller tillgångarna hos den juridiska personen att begära att europeiska digitala identitetsplånböcker omedelbart återkallas.
- (35) För att främja spridningen av europeiska digitala identitetsplånböcker och en bredare användning av digitala identiteter bör medlemsstaterna inte bara främja fördelarna med de relevanta tjänsterna, utan bör även, i samarbete med den privata sektorn, forskare och den akademiska världen, utveckla utbildningsprogram som syftar till att stärka de digitala färdigheterna hos sina medborgare och invånare, särskilt för utsatta grupper, såsom personer med funktionsnedsättning och äldre personer. Medlemsstaterna bör också öka medvetenheten om fördelarna och riskerna med europeiska digitala identitetsplånböcker genom informationskampanjer.
- (36) För att säkerställa att det europeiska ramverket för digital identitet är öppet för innovation och teknisk utveckling och att det är framtidssäkrat uppmantras medlemsstaterna att gemensamt inrätta testmiljöer där innovativa lösningar kan testas i en kontrollerad och säker miljö i syfte att förbättra lösningarnas funktion, personuppgiftsskydd, säkerhet och interoperabilitet och lägga grunden för framtida uppdrag av tekniska referenser och rättsliga krav. Denna miljö bör även uppmantra deltagande av små och medelstora företag, uppstarts företag och enskilda innovatörer och forskare samt berörda parter från branschen. Sådana initiativ bör bidra till och stärka regel efterlevnaden och den tekniska robustheten hos de europeiska digitala identitetsplånböcker som ska tillhandahållas unionsmedborgare och invånare i unionen, och därigenom förhindra att det utvecklas lösningar som inte är förenliga med unionsrätten om dataskydd eller som är sårbara vad gäller säkerheten.
- (37) Genom Europaparlamentets och rådets förordning (EU) 2019/1157⁽¹⁾ kommer säkerheten för identitetskort att utökas med ytterligare säkerhetsdetaljer i augusti 2021. Medlemsstaterna bör överväga om det är möjligt att anmäla dem inom ramen för systemen för elektronisk identifiering för att utöka den gränsöverskridande tillgången till medel för elektronisk identifiering.
- (38) Anmälningen av system för elektronisk identifiering bör förenklas och påskyndas för att främja tillgången till bekväma, tillförlitliga, säkra och innovativa lösningar för autentisering och identifiering och, i förekommande fall, uppmantra privata leverantörer av lösningar för identifiering att erbjuda system för elektronisk identifiering till medlemsstaternas myndigheter för anmälning som nationella system för elektronisk identifiering enligt förordning (EU) nr 910/2014.

⁽¹⁾ Europaparlamentets och rådets förordning (EU) 2019/1157 av den 20 juni 2019 om säkrare identitetskort för unionsmedborgare och uppehållshandlingar som utfärdas till unionsmedborgare och deras familjemedlemmar när de utövar rätten till fri rörlighet (EUT L 188, 12.7.2019, s. 67).

- (39) En effektivisering av de nuvarande förfarandena för anmälan och sakkunnigbedömning kommer att förhindra skilda synsätt på bedömningen av olika anmälda system för elektronisk identifiering och bygga upp förtroendet mellan medlemsstaterna. Nya, förenklade mekanismer är avsedda att främja medlemsstaternas samarbete i frågor som rör säkerheten och interoperabiliteten med avseende på deras anmälda system för elektronisk identifiering.
- (40) Medlemsstaterna bör kunna utnyttja nya, flexibla verktyg för att säkerställa att kraven i denna förordning och i de relevanta genomförandeakter som antas enligt denna uppfylls. Denna förordning bör ge medlemsstaterna möjlighet att använda rapporter och bedömningar, som utförts av ackrediterade organ för bedömning av överensstämmelse, såsom föreskrivs i samband med de certifieringsordningar som ska inrättas på unionsnivå enligt förordning (EU) 2019/881, som stöd i deras arbete med att anpassa systemen, eller delar av dessa, till förordning (EU) nr 910/2014.
- (41) Offentliga tjänsteleverantörer använder de uppgifter för personidentifiering som finns tillgängliga genom systemen för elektronisk identifiering enligt förordning (EU) nr 910/2014 för att matcha den elektroniska identiteten hos användare från andra medlemsstater med de uppgifter för personidentifiering som tillhandahålls dessa användare i den medlemsstat som utför den gränsöverskridande identitetsmatchningsprocessen. För att säkerställa korrekt identitetsmatchning när medlemsstaterna agerar som förlitande parter krävs det dock i många fall, trots användningen av den minimiuppsättning uppgifter som tillhandahålls inom ramen för de anmälda systemen för elektronisk identifiering, ytterligare information om användaren och specifika kompletterande unika identifieringsförfaranden som genomförs på nationell nivå. För att ytterligare stödja användbarheten hos medel för elektronisk identifiering, tillhandahålla bättre offentliga nättjänster och öka rättssäkerheten när det gäller användarnas elektroniska identitet bör förordning (EU) nr 910/2014 kräva att medlemsstaterna vidtar specifika åtgärder online för att säkerställa otvetydig identitetsmatchning när användare avser att få åtkomst till gränsöverskridande offentliga nättjänster.
- (42) Vid utvecklingen av europeiska digitala identitetsplånböcker är det mycket viktigt att ta hänsyn till användarnas behov. Meningsfulla användningsfall och nättjänster som förlitar sig på europeiska digitala identitetsplånböcker bör vara tillgängliga. För användarnas bekvämlighet och för att säkerställa gränsöverskridande tillgång till sådana tjänster är det viktigt att vidta åtgärder för att underlätta en liknande strategi för utformning, utveckling och genomförande av nättjänster i alla medlemsstater. Icke-bindande riktlinjer för hur nättjänster som förlitar sig på europeiska digitala identitetsplånböcker ska utformas, utvecklas och genomföras har potential att bli ett användbart verktyg för att uppnå detta mål. Sådana riktlinjer bör utarbetas med beaktande av unionens interoperabilitetsramverk. Medlemsstaterna bör ha en ledande roll när det gäller att anta dessa riktlinjer.
- (43) I enlighet med Europaparlamentets och rådets direktiv (EU) 2019/882⁽¹⁾ bör personer med funktionsnedsättning kunna använda europeiska digitala identitetsplånböcker, betrodda tjänster och slutanvändarprodukter som används i samband med tillhandahållandet av dessa tjänster på samma villkor som andra användare.
- (44) För att säkerställa en effektiv efterlevnad av denna förordning bör det fastställas en miniminivå för de maximala administrativa sanktionsavgifterna för både kvalificerade och icke-kvalificerade tillhandahållare av betrodda tjänster. Medlemsstaterna bör föreskriva effektiva, proportionella och avskräckande sanktioner. Vid fastställandet av sanktionerna bör vederbörlig hänsyn tas till de berörda enheternas storlek, deras affärsmodeller och överträdelsernas allvar.
- (45) Medlemsstaterna bör fastställa regler om sanktioner för överträdelser såsom direkta eller indirekta metoder som leder till förväxling mellan icke-kvalificerade och kvalificerade betrodda tjänster eller till icke-kvalificerade tillhandahållare av betrodda tjänster missbrukar EU-förtroendemärket. EU-förtroendemärket bör inte användas på villkor som direkt eller indirekt leder till uppfattningen att icke-kvalificerade betrodda tjänster som tillhandahålls av dessa tillhandahållare är kvalificerade.
- (46) Denna förordning bör inte gälla frågor som avser ingående av och giltigheten hos avtal eller andra rättsliga förpliktelser om unionsrätten eller nationell rätt föreskriver vissa formkrav. Den bör inte heller inverka på nationella formkrav avseende offentliga register, i synnerhet inte kommersiella register eller fastighetsregister.

⁽¹⁾ Europaparlamentets och rådets direktiv (EU) 2019/882 av den 17 april 2019 om tillgänglighetskrav för produkter och tjänster (EUT L 151, 7.6.2019, s. 70).

- (47) Tillhandahållandet och användningen av betrodda tjänster och de fördelar detta innebär vad gäller bekvämlighet och rättssäkerhet i samband med gränsoverskridande transaktioner, i synnerhet när kvalificerade betrodda tjänster används, blir allt viktigare för internationell handel och internationellt samarbete. Unionens internationella partner håller på att inrätta tillitsramverk som har inspirerats av förordning (EU) nr 910/2014. För att underlätta erkännandet av kvalificerade betrodda tjänster och deras tillhandahållare kan kommissionen anta genomförandeakter för att fastställa de villkor enligt vilka tillitsramverk i tredjeländer skulle kunna anses vara likvärdiga med tillitsramverket för kvalificerade betrodda tjänster och tillhandahållare av sådana tjänster i denna förordning. En sådan strategi bör komplettera möjligheten till ett ömsesidigt erkännande av betrodda tjänster och tillhandahållare av sådana tjänster som är etablerade i unionen och i tredjeländer i enlighet med artikel 218 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget). Vid fastställandet av de villkor som måste uppfyllas av tillitsramverk i tredjeländer för att anses vara likvärdiga med tillitsramverket för kvalificerade betrodda tjänster och tillhandahållare av sådana tjänster enligt förordning (EU) nr 910/2014, bör även efterlevnaden av de relevanta bestämmelserna i Europaparlamentets och rådets direktiv (EU) 2022/2555⁽¹³⁾ och förordning (EU) 2016/679 säkerställas, liksom användningen av förteckningar över betrodda tjänsteleverantörer som avgörande komponenter för att bygga upp förtroende.
- (48) Denna förordning bör främja valfrihet och möjligheten att byta mellan europeiska digitala identitetsplänböcker om en medlemsstat har godkänt mer än en lösning för europeiska digitala identitetsplänböcker på sitt territorium. För att undvika inläsnings effekter i sådana situationer bör tillhandahållarna av europeiska digitala identitetsplänböcker där detta är tekniskt genomförbart säkerställa effektiv portabilitet för uppgifter på begäran av användare av europeiska digitala identitetsplänböcker, och de bör inte tillåtas använda avtalsenliga, ekonomiska eller tekniska spårar för att förhindra eller försvåra ett effektivt byte mellan olika europeiska digitala identitetsplänböcker.
- (49) För att säkerställa att de europeiska digitala identitetsplänböckerna fungerar korrekt behöver tillhandahållare av europeiska digitala identitetsplänböcker effektiv interoperabilitet och rättvisa, rimliga och icke-diskriminerande villkor för att de europeiska digitala identitetsplänböckerna ska få tillgång till specifika maskinvaru- och programvarufunktioner hos mobila enheter. Dessa komponenter skulle särskilt kunna omfatta NFC-antennor och säkerhetskomponenter, inbegripet universella smartkort, inbyggda säkerhetskomponenter, microSD-kort och Bluetooth Low Energy. Tillgången till komponenterna skulle kunna kontrolleras av mobilnätoperatörer och tillverkare av utrustning. Därför bör tillverkare av originalutrustning för mobila enheter eller tillhandahållare av elektroniska kommunikationstjänster inte neka tillgång till sådana komponenter när de behövs för att tillhandahålla tjänster relaterade till de europeiska digitala identitetsplänböckerna. Dessutom bör de företag som betecknas som grindvakter för centrala plattformstjänster enligt kommissionens förteckning i Europaparlamentets och rådets förordning (EU) 2022/1925⁽¹⁴⁾ fortsätta att omfattas av de särskilda bestämmelserna i den förordningen, på grundval av artikel 6.7 i den förordningen.
- (50) För att anpassa de skyldigheter avseende cybersäkerhet som införts för tillhandahållare av betrodda tjänster, och för att dessa tillhandahållare och deras respektive behöriga myndigheter ska kunna gynnas av den rättsliga ram som inrättas genom direktiv (EU) 2022/2555, ska betrodda tjänster vidta lämpliga tekniska och organisatoriska åtgärder i enlighet med det direktivet, däribland åtgärder mot systembrister, mänskliga fel, olagliga handlingar eller naturfenomen, för att hantera säkerhetsriskerna i de nätverk och informationssystem som dessa tillhandahållare använder för att tillhandahålla sina tjänster, liksom för att anmäla allvarliga incidenter och cyberhot i enlighet med det direktivet. När det gäller rapporteringen av incidenter bör tillhandahållare av betrodda tjänster anmäla varje incident som har en betydande inverkan på tillhandahållandet av deras tjänster, däribland sådana som orsakas av stöld eller förlust av anordningar, skador på nätverkskablar eller incidenter i samband med identifieringen av personer. Kraven och rapporteringsskyldigheterna för hanteringen av riskerna för cybersäkerheten enligt direktiv (EU) 2022/2555 bör ses som komplement till de krav som införts för tillhandahållare av betrodda tjänster enligt denna förordning. I tillämpliga fall bör nationella förfaranden eller riktlinjer som fastställts med avseende på genomförandet av säkerhets- och rapporteringskraven och övervakningen av efterlevnaden av sådana krav enligt förordning (EU) nr 910/2014 fortsätta att tillämpas av de behöriga myndigheter som utses enligt direktiv (EU) 2022/2555. Denna förordning påverkar inte skyldigheten att anmäla personuppgiftsincidenter enligt förordning (EU) 2016/679.

⁽¹³⁾ Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972, och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet) (EUT L 333, 27.12.2022, s. 80).

⁽¹⁴⁾ Europaparlamentets och rådets förordning (EU) 2022/1925 av den 14 september 2022 om öppna och rättvisa marknader inom den digitala sektorn och om ändring av direktiv (EU) 2019/1937 och (EU) 2020/1828 (förordningen om digitala marknader) (EUT L 265, 12.10.2022, s. 1).

- (51) Vederbörlig hänsyn bör tas för att säkerställa ett effektivt samarbete mellan de tillsynsorgan som utses i enlighet med artikel 46b i förordning (EU) nr 910/2014 och de behöriga myndigheter som utses eller fastställs i enlighet med artikel 8.1 i direktiv (EU) 2022/2555. Om ett sådant tillsynsorgan skiljer sig från en sådan behörig myndighet bör de bedriva ett nära och effektivt samarbete genom att utbyta relevant information för att säkerställa en effektiv tillsyn och att tillhandahållarna av betrodda tjänster uppfyller kraven i förordning (EU) nr 910/2014 och direktiv (EU) 2022/2555. I synnerhet bör de tillsynsorganen som utses i enlighet med förordning (EU) nr 910/2014 ha rätt att begära att behöriga myndigheter som utses eller fastställs i enlighet med direktiv (EU) 2022/2555 tillhandahåller all relevant information som behövs för att bevilja status som kvalificerad och för att utföra tillsynsåtgärder för att kontrollera att tillhandahållarna av betrodda tjänster uppfyller de relevanta kraven i direktiv (EU) 2022/2555 eller kräva att de åtgärder bristerna.
- (52) Det är av avgörande betydelse att det föreskrivs en rättslig ram för att främja gränsöverskridande erkännande mellan befintliga nationella rättssystem för elektroniska tjänster för rekommenderade leveranser. En sådan ram kan även skapa nya marknads möjligheter för tillhandahållare av betrodda tjänster i unionen att erbjuda nya unionsomfattande elektroniska tjänster för rekommenderade leveranser. För att säkerställa att data som skickas med hjälp av en kvalificerad elektronisk tjänst för rekommenderade leveranser levereras till rätt adressat bör kvalificerade elektroniska tjänster för rekommenderade leveranser med komplett säkerhet säkerställa identifieringen av adressaten, medan en hög tillförlitlighetsnivå skulle räcka när det gäller identifiering av avsändaren. Tillhandahållare av kvalificerade elektroniska tjänster för rekommenderade leveranser bör av medlemsstaterna uppmanas att göra sina tjänster interoperabla med sådana kvalificerade elektroniska tjänster för rekommenderade leveranser som tillhandahålls av andra kvalificerade tillhandahållare av betrodda tjänster i syfte att enkelt överföra elektroniska rekommenderade uppgifter mellan två eller flera kvalificerade tillhandahållare av betrodda tjänster och främja god sed på den inre marknaden.
- (53) I de flesta fall kan unionsmedborgare och invånare i unionen inte utbyta digital information över gränserna om sin identitet, t.ex. adress, ålder och yrkeskvalifikationer, körkort och andra tillstånd eller betalningsuppgifter, på ett säkert sätt och med en hög nivå av dataskydd.
- (54) Det bör vara möjligt att utfärda och hantera tillförlitliga elektroniska attribut och bidra till att minska den administrativa bördan genom att ge unionsmedborgare och invånare i unionen möjlighet att använda dem i privata och offentliga transaktioner. Unionsmedborgare och invånare i unionen bör till exempel kunna bevisa innehav av ett giltigt körkort som har utfärdats av en myndighet i en medlemsstat och som kan verifieras och godtas av de berörda myndigheterna i andra medlemsstater. De bör även kunna förlita sig på sina uppgifter om social trygghet eller framtida digitala resehandlingar i ett gränsöverskridande sammanhang.
- (55) Alla tillhandahållare av tjänster som utfärdar attesterade attribut i elektroniskt format, såsom examensbevis, licenser, personbevis eller befogenheter och uppdrag att företräda fysiska eller juridiska personer eller agera på deras vägnar bör anses vara en tillhandahållare av betrodda elektroniska attributsintyg. Ett elektroniskt attributsintyg bör inte förvägras rättslig verkan på grund av att det har elektronisk form eller inte uppfyller kraven för ett kvalificerat elektroniskt attributsintyg. Allmänna krav bör fastställas för att säkerställa att kvalificerade elektroniska attributsintyg har samma rättsliga verkan som lagligen utfärdade intyg i pappersform. Sådana krav bör emellertid gälla utan att det påverkar tillämpningen av unionsrätt eller nationell rätt som omfattar ytterligare sektorspecifika krav med underliggande rättsliga verkningar vad gäller formen och, i synnerhet, det gränsöverskridande erkännandet av kvalificerade elektroniska attributsintyg i tillämpliga fall.
- (56) En bred tillgång till och användbarhet för europeiska digitala identitetsplånböcker bör leda till att de godtas i större utsträckning och öka förtroendet för dem både hos privatpersoner och hos privata tillhandahållare av tjänster. Privata förlitande parter som tillhandahåller tjänster till exempel inom områdena transport, energi, bankväsende och finansiella tjänster, social trygghet, hälso- och sjukvård, dricksvatten, posttjänster, digital infrastruktur, telekommunikation eller utbildning bör därför godtas att de europeiska digitala identitetsplånböckerna används i samband med tillhandahållandet av tjänster där en säker autentisering för onlineidentifiering krävs enligt unionsrätten eller nationell rätt eller genom avtalsenliga skyldigheter. Varje begäran som den förlitande parten framställer om information från användaren av en europeisk digital identitetsplånbok bör vara nödvändig för och stå i proportion till den avsedda användningen i ett givet fall, bör vara förenlig med principen om uppgiftsminimering och bör säkerställa transparens när det gäller vilka uppgifter som delas och för vilka ändamål. För att underlätta användningen och godtagandet av europeiska digitala identitetsplånböcker bör allmänt accepterade branschstandarder och specifikationer beaktas när plånböckerna införs.

- (57) Om mycket stora onlineplattformar, enligt artikel 33.1 i Europaparlamentets och rådets förordning (EU) 2022/2065⁽¹⁾, kräver att användarna är autentiserade för att få tillgång till nättjänster bör dessa plattformar vara skyldiga att godta användning av europeiska digitala identitetsplånböcker på användarens frivilliga begäran. Användarna bör inte vara tvungna att använda en europeisk digital identitetsplånbok för att få tillgång till privata tjänster, och deras tillgång till tjänster bör inte begränsas eller hindras på grund av att de inte använder en europeisk digital identitetsplånbok. Om användarna emellertid vill göra det, bör stora onlineplattformar godta dem i detta syfte, med iakttagande av principen om uppgiftsminimering och användarnas rätt att använda pseudonymer som de föredrar. Med tanke på de mycket stora onlineplattformarnas räckvidd, i synnerhet när det gäller antalet mottagare av tjänster och antalet ekonomiska transaktioner, är skyldigheten att godta europeiska digitala identitetsplånböcker nödvändig för att öka användarnas skydd mot bedrägerier och säkerställa en hög nivå av dataskydd.
- (58) Uppförandekoder på unionsnivå bör utarbetas för att bidra till allmän tillgång till och användbarhet hos medel för elektronisk identifiering, däribland de europeiska digitala identitetsplånböckerna, inom denna förordnings tillämpningsområde. Uppförandekoderna bör underlätta ett brett erkännande av medel för elektronisk identifiering, däribland europeiska digitala identitetsplånböcker, bland de tjänsteleverantörer som inte klassificeras som mycket stora plattformar och som förlitar sig på tredje parts tjänster för elektronisk identifiering för användarautentisering.
- (59) Selektivt utlämnande är ett begrepp som ger dataägaren rätt att endast lämna ut vissa delar av en större datamängd, så att den mottagande enheten endast kan inhämta information som är nödvändig för tillhandahållandet av en tjänst som begärs av en användare. De europeiska digitala identitetsplånböckerna bör ha tekniska egenskaper som möjliggör ett selektivt utlämnande av attribut till förlitande parter. Det bör vara tekniskt möjligt för användaren att selektivt utlämna attribut, inbegripet från flera olika elektroniska inlysningsobjekt, och att kombinera och presentera dem sömlöst för förlitande parter. Denna funktion bör vara grundläggande inbyggd i europeiska digitala identitetsplånböcker som förstärker bekvämligheten och skyddet av personuppgifter, inbegripet uppgiftsminimering.
- (60) Såvida inte särskilda bestämmelser i unionsrätten eller nationell rätt kräver att användarna ska identifiera sig bör åtkomst till tjänster med hjälp av en pseudonym inte förbjudas.
- (61) Attribut som tillhandahålls av kvalificerade tillhandahållare av betrodda tjänster som en del av kvalificerade attributsinlysningsobjekt bör verifieras mot autentiska källor, antingen direkt av den kvalificerade tillhandahållaren av betrodda tjänster eller genom särskilt utsedda mellanhänder som erkänns på nationell nivå i enlighet med unionsrätten eller nationell rätt för ett säkert utbyte av inlysningsobjekt mellan tillhandahållare av identitetslösningar eller attributsinlysningsobjekt och förlitande parter. Medlemsstaterna bör inrätta lämpliga mekanismer på nationell nivå för att säkerställa att sådana kvalificerade tillhandahållare av betrodda tjänster som utfärdar kvalificerade elektroniska attributsinlysningsobjekt kan kontrollera, på grundval av samtycke från den person till vilken inlysningsobjektet utfärdas, äktheten hos de attribut som byggs på autentiska källor. Lämpliga mekanismer bör kunna innefatta användningen av särskilda mellanhänder eller tekniska lösningar som i enlighet med nationell rätt ger tillgång till de autentiska källorna. Säkerställandet av tillgång till en mekanism som möjliggör kontroll av attribut mot autentiska källor avser att underlätta för kvalificerade tillhandahållare av betrodda tjänster som utfärdar kvalificerade elektroniska attributsinlysningsobjekt att uppfylla sina skyldigheter enligt förordning (EU) nr 910/2014. En ny bilaga till den förordningen bör innehålla en förteckning över kategorier av attribut avseende vilka medlemsstaterna ska säkerställa att åtgärder vidtas för att göra det möjligt för kvalificerade tillhandahållare av elektroniska attributsinlysningsobjekt att på användarens begäran på elektronisk väg kontrollera deras äkthet gentemot den relevanta autentiska källan.
- (62) Säker elektronisk identifiering och tillhandahållande av attributsinlysningsobjekt bör erbjuda ytterligare flexibilitet och lösningar inom sektorn för finansiella tjänster för att göra det möjligt att identifiera kunder och utbyta särskilda attribut som behövs för att, till exempel, uppfylla kraven på kundkontroll enligt en framtida förordning om inrättande av myndigheten för bekämpning av penningtvätt och lämplighetskraven i lagstiftningen om investerarskydd, eller för att bidra till efterlevnaden av kraven på stark kundautentisering för onlineidentifiering vid kontoinloggning och inledande av transaktioner inom betalningstjänstområdet.
- (63) Den rättsliga verkan av en elektronisk underskrift ska inte bestridas på den grunden att den är i elektronisk form eller inte uppfyller kraven för en kvalificerad elektronisk underskrift. Det är dock i nationell rätt som den rättsliga verkan av elektroniska underskrifter ska fastställas, med undantag för de krav som föreskrivs i denna förordning, enligt vilka den rättsliga verkan av en kvalificerad elektronisk underskrift ska anses vara likvärdig med en handskrivnen

⁽¹⁾ Europaparlamentets och rådets förordning (EU) 2022/2065 av den 19 oktober 2022 om en inre marknad för digitala tjänster och om ändring av direktiv 2000/31/EG (förordningen om digitala tjänster) (EUT L 277, 27.10.2022, s. 1).

underskrift. Vid fastställandet av elektroniska underskrifters rättsliga verkan bör medlemsstaterna beakta principen om proportionalitet mellan det rättsliga värdet av en handling som ska undertecknas och den säkerhetsnivå och kostnad som en elektronisk underskrift kräver. För att öka tillgängligheten till och användningen av elektroniska underskrifter uppmanas medlemsstaterna att överväga användningen av avancerade elektroniska underskrifter för de dagliga transaktioner för vilka de tillhandahåller en tillräcklig nivå av säkerhet och tillförlitlighet.

- (64) För att säkerställa enhetliga certifieringsmetoder i hela unionen bör kommissionen utfärda riktlinjer för certifiering och omcertifiering av kvalificerade anordningar för skapande av elektroniska underskrifter och kvalificerade anordningar för skapande av elektroniska stämplatser, inbegripet vad gäller deras giltighet och tidsbegränsningar. Denna förordning hindrar inte de offentliga eller privata organ som har certifierade kvalificerade anordningar för skapande av elektroniska underskrifter från att omcertifiera sådana anordningar för en kort certifieringsperiod, baserat på resultaten av den föregående certifieringsprocessen, om en sådan omcertifiering inte kan utföras inom den rättsligt fastställda tidsramen av ett annat skäl än en säkerhetsincident, utan att det påverkar skyldigheten att utföra en sårbarhetsbedömning och utan att det påverkar tillämplig certifieringspraxis.
- (65) Utfärdandet av certifikat för autentisering av webbplatser är avsett att ge användarna tillit, med en hög tillförlitlighetsnivå när det gäller identiteten hos den enhet som står bakom webbplatsen, oavsett vilken plattform som används för att visa identiteten. Dessa certifikat bör bidra till att bygga upp förtroendet för näthandeln, eftersom användarna kan förväntas hysa tillit till en webbplats som har autentiserats. Användningen av sådana certifikat bör vara frivillig. För att autentiseringen av webbplatser ska kunna bli ett sätt att stärka förtroendet, ge användaren en bättre upplevelse och främja tillväxten på den inre marknaden fastställs i denna förordning ett tillitsramverk som innefattar minimiskyldigheter vad gäller säkerhet och skadeståndsansvar för tillhandahållare av kvalificerade certifikat för autentisering av webbplatser och krav i fråga om utfärdandet av dessa certifikat. Nationella förteckningar över betrodda tjänsteleverantörer bör bekräfta att tjänster för autentisering av webbplatser och deras tillhandahållare av betrodda tjänster har status som kvalificerade, inbegripet att de fullt ut följer kraven i denna förordning när det gäller utfärdande av kvalificerade certifikat för autentisering av webbplatser. Erkännandet av kvalificerade certifikat för autentisering av webbplatser innebär att tillhandahållare av webbplatser inte bör neka äktheten hos kvalificerade certifikat för autentisering av webbplatser vars enda i syfte är att intyga kopplingen mellan webbplatsens domännamn och den fysiska eller juridiska person till vilken certifikatet är utfärdat eller bekräfta den personens identitet. Tillhandahållare av webbplatser bör visa de certifierade identitetsuppgifterna och de andra intygade attributen för slutanvändaren på ett användarvänligt sätt i webbplasmiljön genom valfria tekniska medel. För detta ändamål bör tillhandahållare av webbplatser säkerställa stöd och interoperabilitet med kvalificerade certifikat för autentisering av webbplatser som utfärdats i fullständig överensstämmelse med denna förordning. Den skyldighet som innebär erkännande av och kompatibilitet med samt stöd för kvalificerade certifikat för autentisering av webbplatser påverkar inte friheten för tillhandahållare av webbplatser att säkerställa webbsäkerhet, domänautentisering och kryptering av webbttrafik på ett sätt och med hjälp av den teknik som de anser lämpligast. För att bidra till slutanvändarnas onlinesäkerhet bör tillhandahållare av webbplatser i undantagsfall kunna vidta säkerhetsåtgärder som är både nödvändiga och proportionella som en reaktion på vägrundade farhågor om säkerhetsincidenter eller integritetsförluster hos ett identifierat certifikat eller en identifierad uppsättning certifikat. Om tillhandahållare av webbplatser vidtar sådana säkerhetsåtgärder bör de, utan onödigt dröjsmål, underrätta kommissionen, det nationella tillsynsorganet om vilken enhet certifikatet utfärdades till och vilken kvalificerad tillhandahållare av betrodda tjänster som utfärdade certifikatet eller uppsättningen certifikat, om alla farhågor med avseende på en sådan säkerhetsincident eller integritetsförlust samt om vilka åtgärder som vidtagits avseende det enskilda certifikatet eller uppsättningen certifikat. Dessa åtgärder bör inte påverka den skyldighet som tillhandahållare av webbplatser har att erkänna kvalificerade certifikat för autentisering av webbplatser i enlighet med de nationella förteckningarna över betrodda tjänsteleverantörer. För att ytterligare skydda unionsmedborgare och invånare i unionen och främja användningen av kvalificerade certifikat för autentisering av webbplatser bör medlemsstaternas offentliga myndigheter överväga att införa kvalificerade certifikat för autentisering av webbplatser på sina egna webbplatser. De åtgärder som föreskrivs i denna förordning som syftar till att skapa ökad samstämmighet mellan medlemsstaternas skilda tillvägagångssätt och praxis när det gäller tillsynsförfaranden är avsedda att bidra till större förtroende och tillit för säkerhet, kvalitet och tillgänglighet avseende kvalificerade certifikat för autentisering av webbplatser.
- (66) Många medlemsstater har infört nationella krav för tjänster som tillhandahåller säker och tillförlitlig elektronisk arkivering för att möjliggöra långsiktig lagring av elektroniska uppgifter och elektroniska dokument och tillhörande betrodda tjänster. För att säkerställa rättssäkerhet, förtroende och harmonisering mellan medlemsstaterna bör en rättslig ram för kvalificerade elektroniska arkiverings tjänster inrättas, och den bör inspireras av ramen för de andra betrodda tjänster som föreskrivs i denna förordning. Den rättsliga ramen för kvalificerade elektroniska arkiverings tjänster bör erbjuda tillhandahållare och användare av betrodda tjänster en effektiv verktygslåda som omfattar funktionskrav för den elektroniska arkiverings tjänsten samt tydlig rättslig verkan när en kvalificerad elektronisk arkiverings tjänst används. Bestämmelserna bör vara tillämpliga på elektroniska uppgifter och elektroniska dokument skapade i elektronisk form liksom på pappersdokument som har skannats och digitaliserats.

När så krävs bör bestämmelserna tillåta att bevarade elektroniska uppgifter och elektroniska dokument överförs till olika medier eller format i syfte att förlänga deras hållbarhet och läsbarhet bortom den tekniska giltighetstiden, samtidigt som förluster och ändringar förhindras i möjligaste mån. När elektroniska data och elektroniska dokument som lämnas till den elektroniska arkiveringstjänsten innehåller en eller flera kvalificerade elektroniska underskrifter eller kvalificerade elektroniska stämplarna bör tjänsten använda förfaranden och teknik som kan förlänga deras tillförlitlighet under bevarandeperioden för sådana uppgifter, eventuellt genom användning av andra kvalificerade betrodda tjänster som inrättas genom denna förordning. För att skapa bevarandebevis när elektroniska underskrifter, elektroniska stämplarna eller elektroniska tidsstämplingar används bör kvalificerade betrodda tjänster användas. I den mån som elektroniska arkiveringstjänster inte harmoniseras genom denna förordning bör medlemsstaterna kunna behålla eller införa nationella bestämmelser, i enlighet med unionsrätten, som rör dessa tjänster, såsom särskilda bestämmelser för tjänster som är integrerade i en organisation och som endast används för den organisationens interna arkiv. Denna förordning bör inte göra skillnad på elektroniska uppgifter och elektroniska dokument skapade i elektronisk form och fysiska dokument som har digitaliserats.

- (67) Nationella arkiv och minnesinstitutioners verksamhet regleras, i egenskap av organisationer som arbetar med att bevara det dokumenterade arvet i allmänhetens intresse, vanligtvis i nationell rätt och tillhandahåller inte nödvändigtvis betrodda tjänster i den mening som avses i denna förordning. I den mån sådana institutioner inte tillhandahåller sådana betrodda tjänster ska denna förordning inte påverka deras verksamhet.
- (68) Elektroniska liggare är en sekvens av elektroniska dataloggar som bör säkerställa dataintegriteten och riktigheten i deras kronologiska ordning. Elektroniska liggare bör upprätta en kronologisk sekvens av dataloggar. Tillsammans med annan teknik bör de bidra till lösningar för effektivare och omdanande offentliga tjänster såsom elektronisk röstning, gränsöverskridande samarbete mellan tullmyndigheter, gränsöverskridande samarbete mellan akademiska institutioner och registrering av äganderätt till fastigheter i decentraliserade fastighetsregister. Kvalificerade elektroniska liggare bör skapa en legal presumtion för den unika och korrekta sekventiella kronologiska ordningsföljden och integriteten hos dataloggarna i liggaren. På grund av sina specifika egenskaper, såsom den sekventiella kronologiska ordningsföljden för dataloggar, bör elektroniska liggare skiljas från andra betrodda tjänster såsom elektroniska tidsstämplingar och elektroniska tjänster för rekommenderade leveranser. För att säkerställa rättssäkerhet och främja innovation bör en unionsomfattande rättslig ram inrättas som föreskriver ett gränsöverskridande erkännande av betrodda tjänster för registrering av uppgifter i elektroniska liggare. Detta bör i tillräcklig utsträckning kunna förhindra att samma digitala tillgång kopieras och säljs mer än en gång till olika parter. Processen för att skapa och uppdatera en elektronisk liggare beror på vilken typ av liggare som används, nämligen om den är centraliserad eller distribuerad. Denna förordning bör säkerställa teknikneutralitet, dvs. varken gynna eller diskriminera någon teknik som används för att genomföra den nya betrodda tjänsten för elektroniska liggare. Dessutom bör hållbarhetsindikatorer för eventuella negativa effekter på klimatet eller andra miljörelaterade negativa effekter beaktas av kommissionen, med hjälp av lämpliga metoder, när den utarbetar de genomförandeakter där kraven för kvalificerade elektroniska liggare specificeras.
- (69) Rollen för tillhandahållare av betrodda tjänster för elektroniska liggare bör vara att säkerställa den sekventiella registreringen av uppgifter i liggaren. Denna förordning påverkar inte eventuella rättsliga skyldigheter som användare av elektroniska liggare har enligt unionsrätten eller nationell rätt. Till exempel bör användningsfall som inbegriper behandlingen av personuppgifter uppfylla kraven i förordning (EU) 2016/679 och användningsfall som rör finansiella tjänster bör uppfylla kraven i relevant unionsrätt om finansiella tjänster.
- (70) För att undvika fragmentering och hinder på den inre marknaden på grund av varierande standarder och tekniska begränsningar, och för att säkerställa en samordnad process för att undvika att genomförandet av det europeiska ramverket för digital identitet påverkas, krävs det ett förfarande för ett nära och strukturerat samarbete mellan kommissionen, medlemsstaterna, civilsamhället, den akademiska världen och den privata sektorn. För att uppnå detta mål bör medlemsstaterna och kommissionen samarbeta inom den ram som fastställs i kommissionens rekommendation (EU) 2021/946⁽¹⁶⁾ för att utarbeta en unionsgemensam verktygslåda för det europeiska ramverket för digital identitet. I detta sammanhang bör medlemsstaterna enas om en övergripande teknisk arkitektur och referensram, ett antal gemensamma standarder och tekniska referenser inbegripet erkända befintliga standarder samt en uppsättning riktlinjer och beskrivningar av bästa praxis som åtminstone omfattar all funktionalitet och interoperabilitet hos europeiska digitala identitetsplånböcker, inklusive elektroniska underskrifter, och hos tillhandahållaren av kvalificerade betrodda tjänster för elektroniska attributsintyg som fastställs i denna förordning. I detta sammanhang bör medlemsstaterna även komma överens om gemensamma inslag i en affärsmodell och en avgiftsstruktur för europeiska digitala identitetsplånböcker för att underlätta användningen, i synnerhet för små och

⁽¹⁶⁾ Kommissionens rekommendation (EU) 2021/946 av den 3 juni 2021 om en unionsgemensam verktygslåda för en samordnad strategi för en europeisk ram för digital identitet (EUT L 210, 14.6.2021, s. 51).

medelstora företag i gränsöverskridande sammanhang. Innehållet i verktygslådan bör utvecklas parallellt med och återspegla resultatet av diskussionen och processen för antagandet av det europeiska ramverket för digital identitet.

- (71) Denna förordning föreskriver en harmoniserad nivå av kvalitet, tillförlitlighet och säkerhet när det gäller kvalificerade betrodda tjänster, oavsett var verksamheten bedrivs. En kvalificerad tillhandahållare av betrodda tjänster bör därför ha rätt att lägga ut sin verksamhet vad gäller tillhandahållandet av en kvalificerad betrodd tjänst på entreprenad i ett tredje land, om det tredje landet tillhandahåller tillräckliga garantier och säkerställer att tillsynsverksamhet och revisioner kan verkställas som om de hade bedrivits i unionen. Om efterlevnaden av denna förordning inte kan garanteras fullt ut bör tillsynsorganen kunna vidta proportionella och motiverade åtgärder, inbegripet återkallande av den tillhandahållna betrodda tjänstens status som kvalificerad.
- (72) För att säkerställa rättssäkerhet vad gäller giltigheten för avancerade elektroniska underskrifter baserade på kvalificerade certifikat är det viktigt att bedömningen av den förlitande part som utför valideringen av den avancerade elektroniska underskriften baserad på kvalificerade certifikat specificeras.
- (73) Tillhandahållare av betrodda tjänster bör använda krypteringsmetoder som återspeglar rådande bästa praxis och tillförlitliga tillämpningar av dessa algoritmer för att säkerställa säkerheten och tillförlitligheten hos sina betrodda tjänster.
- (74) I denna förordning fastställs en skyldighet för kvalificerade tillhandahållare av betrodda tjänster att kontrollera identiteten på en fysisk eller juridisk person till vilken det kvalificerade certifikatet eller det kvalificerade elektroniska attributsintyget utfärdas på grundval av olika harmoniserade metoder i hela unionen. För att säkerställa att kvalificerade certifikat och kvalificerade elektroniska attributsintyg utfärdas till den person som de tillhör och att de intygar den korrekta och unika uppsättning uppgifter som representerar den personens identitet, bör kvalificerade tillhandahållare av betrodda tjänster som utfärdar kvalificerade certifikat eller utfärdar kvalificerade elektroniska attributsintyg, vid tidpunkten för utfärdandet av dessa certifikat och intyg med full säkerhet säkerställa identifieringen av den personen. Utöver den obligatoriska kontrollen av personens identitet, i tillämpliga fall för utfärdande av kvalificerade certifikat och vid utfärdande av ett kvalificerat elektroniskt attributsintyg, bör kvalificerade tillhandahållare av betrodda tjänster med full säkerhet säkerställa att de intygade attributen för den person till vilken det kvalificerade certifikatet eller det kvalificerade elektroniska attributsintyget utfärdas är korrekta och riktiga. Dessa krav på resultat och full säkerhet vid kontrollen av de intygade uppgifterna bör stödjas på lämpligt sätt, bland annat genom användning av en eller, när så krävs, en kombination av specifika metoder som föreskrivs i denna förordning. Det bör vara möjligt att kombinera dessa metoder för att ge en lämplig grund för kontroll av identiteten på den person till vilken det kvalificerade certifikatet eller ett kvalificerat elektroniskt attributsintyg utfärdas. En sådan kombination bör kunna innefatta användning av medel för elektronisk identifiering som uppfyller kraven på tillförlitlig väsentlig i kombination med andra metoder för identitetskontroll som skulle göra det möjligt att uppfylla de harmoniserade kraven i denna förordning vad gäller tillförlitlig hög som en del av ytterligare harmoniserade distansförfaranden och säkerställa identifiering med en hög tillförlitlighetsnivå. Dessa metoder bör inbegripa möjligheten för den kvalificerade tillhandahållare av betrodda tjänster som utfärdar ett kvalificerat elektroniskt attributsintyg att kontrollera de attribut som ska intygas på elektronisk väg på användarens begäran, i enlighet med unionsrätten eller nationell rätt, inbegripet mot autentiska källor.
- (75) För att hålla denna förordning i linje med den globala utvecklingen och för att följa praxis på den inre marknaden bör de delegerade akter och genomförandeakter som antas av kommissionen ses över och vid behov uppdateras regelbundet. Vid bedömningen av behovet av dessa uppdateringar bör hänsyn tas till ny teknik och nya metoder, standarder eller tekniska specifikationer.
- (76) Eftersom målen för denna förordning, nämligen utvecklingen av det unionsomfattande europeiska ramverket för digital identitet och av ett ramverk för betrodda tjänster, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare, på grund av deras omfattning och verkningar, kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen. I enlighet med proportionalitetsprincipen i samma artikel går denna förordning inte utöver vad som är nödvändigt för att uppnå dessa mål.
- (77) Europeiska datatillsynsmannen har hörts i enlighet med artikel 42.1 i förordning (EU) 2018/1725.

(78) Förordning (EU) nr 910/2014 bör därför ändras i enlighet med detta.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Ändringar av förordning (EU) nr 910/2014

Förordning (EU) nr 910/2014 ska ändras på följande sätt:

1. Artikel 1 ska ersättas med följande:

"Artikel 1

Innehåll

Denna förordning syftar till att säkerställa en väl fungerande inre marknad och tillhandahålla en lämplig säkerhetsnivå för medel för elektronisk identifiering och betrodda tjänster som används i hela unionen i syfte att möjliggöra och underlätta fysiska och juridiska personers utövande av rätten att delta i det digitala samhället på ett säkert sätt och att ha tillgång till offentliga och privata nättjänster i hela unionen. För dessa ändamål fastställs i denna förordning

- a) de villkor enligt vilka medlemsstaterna ska erkänna fysiska och juridiska personers medel för elektronisk identifiering som omfattas av en annan medlemsstats anmälda system för elektronisk identifiering och tillhandahålla och erkänna europeiska digitala identitetsplånböcker,
- b) regler för betrodda tjänster, i synnerhet för elektroniska transaktioner,
- c) en rättslig ram för elektroniska underskrifter, elektroniska stämplatser, elektronisk tidsstämpling, elektroniska dokument, elektroniska tjänster för rekommenderade leveranser, certifikattjänster för autentisering av webbplatser, elektronisk arkivering och elektroniska attributsintyg, anordningar för skapande av elektroniska underskrifter, anordningar för skapande av elektroniska stämplatser samt elektroniska liggare."

2. Artikel 2 ska ändras på följande sätt:

a) Punkt 1 ska ersättas med följande:

"1. Denna förordning är tillämplig på system för elektronisk identifiering som har anmälts av en medlemsstat, på europeiska digitala identitetsplånböcker som tillhandahålls av en medlemsstat och på tillhandahållare av betrodda tjänster som är etablerade inom unionen."

b) Punkt 3 ska ersättas med följande:

"3. Denna förordning påverkar inte unionsrätt eller nationell rätt som avser ingående av avtal och avtalens giltighet eller andra rättsliga eller förfarandemässiga skyldigheter avseende form, eller sektorsspecifika krav avseende form.

4. Denna förordning påverkar inte tillämpningen av Europaparlamentets och rådets förordning (EU) 2016/679 (*).

(*) Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1)."

3. Artikel 3 ska ändras på följande sätt:

a) Leden 1–5 ska ersättas med följande:

"1. *elektronisk identifiering*: en process inom vilken uppgifter för personidentifiering i elektronisk form, som unikt avser en fysisk eller juridisk person eller en fysisk person som företräder en annan fysisk person eller en juridisk person, används.

2. *medel för elektronisk identifiering*: en materiell och/eller immateriell enhet som innehåller uppgifter för personidentifiering och som används för autentisering för en nättjänst eller, i tillämpliga fall, för en offlinetjänst.
3. *uppgifter för personidentifiering*: en uppsättning uppgifter som utfärdas i enlighet med unionsrätten eller nationell rätt, som gör det möjligt att fastställa identiteten på en fysisk eller juridisk person eller på en fysisk person som företräder en annan fysisk person eller en juridisk person.
4. *system för elektronisk identifiering*: ett system för elektronisk identifiering genom vilket medel för elektronisk identifiering utfärdas till en fysisk eller juridisk person eller en fysisk person som företräder en annan fysisk person eller en juridisk person.
5. *autentisering*: en elektronisk process som gör det möjligt att bekräfta en fysisk eller juridisk persons elektroniska identifiering eller att bekräfta ursprunget för och integriteten hos uppgifter i elektronisk form."

b) Följande led ska införas:

"5a. *användare*: en fysisk eller juridisk person, eller en fysisk person som företräder en annan fysisk person eller en juridisk person, som använder betrodda tjänster eller medel för elektronisk identifiering som tillhandahålls i enlighet med denna förordning."

c) Led 6 ska ersättas med följande:

"6. *förlitande part*: en fysisk eller juridisk person som förlitar sig på elektronisk identifiering, europeiska digitala identitetsplånböcker eller andra medel för elektronisk identifiering eller på en betrodd tjänst."

d) Led 16 ska ersättas med följande:

"16. *betrodd tjänst*: en elektronisk tjänst som vanligen tillhandahålls mot ersättning och som består av något av följande:

- a) Utfärdande av certifikat för elektroniska underskrifter, certifikat för elektroniska stämplarna, certifikat för autentisering av webbplatser eller certifikat för tillhandahållande av andra betrodda tjänster.
- b) Validering av certifikat för elektroniska underskrifter, certifikat för elektroniska stämplarna, certifikat för autentisering av webbplatser eller certifikat för tillhandahållande av andra betrodda tjänster.
- c) Skapande av elektroniska underskrifter eller elektroniska stämplarna.
- d) Validering av elektroniska underskrifter eller elektroniska stämplarna.
- e) Bevarande av elektroniska underskrifter, elektroniska stämplarna, certifikat för elektroniska underskrifter eller certifikat för elektroniska stämplarna.
- f) Förvaltning av anordningar för skapande av elektroniska underskrifter på distans eller anordningar för skapande av elektroniska stämplarna på distans.
- g) Utfärdande av elektroniska attributsintyg.
- h) Validering av elektroniska attributsintyg.
- i) Skapande av elektroniska tidsstämplingar.
- j) Validering av elektroniska tidsstämplingar.
- k) Tillhandahållande av elektroniska tjänster för rekommenderade leveranser.
- l) Validering av data som överförs via elektroniska tjänster för rekommenderade leveranser och tillhörande bevis.
- m) Elektronisk arkivering av elektroniska uppgifter och elektroniska dokument.

- n) Registrering av elektroniska uppgifter i en elektronisk liggare.”
- e) Led 18 ska ersättas med följande:
- ”18. *organ för bedömning av överensstämmelse*: ett organ för bedömning av överensstämmelse enligt definitionen i artikel 2.13 i förordning (EG) nr 765/2008 som i enlighet med den förordningen är ackrediterat som behörigt att utföra bedömning av överensstämmelse av en kvalificerad tillhandahållare av en betrodd tjänst och den kvalificerade betrodda tjänst som denne tillhandahåller, eller som behörigt att utföra certifiering av europeiska digitala identitetsplånböcker eller medel för elektronisk identifiering.”
- f) Led 21 ska ersättas med följande:
- ”21. *produkt*: maskinvara eller programvara, eller relevanta komponenter i maskinvara eller programvara, som är avsedda att användas för tillhandahållande av elektronisk identifiering och betrodda tjänster.”
- g) Följande led ska läggas till:
- ”23a. *kvalificerad anordning för skapande av elektroniska underskrifter på distans*: en kvalificerad anordning för skapande av elektroniska underskrifter som förvaltas av en kvalificerad tillhandahållare av betrodda tjänster i enlighet med artikel 29a för undertecknarens räkning.
- 23b. *kvalificerad anordning för skapande av elektroniska stämplor på distans*: en kvalificerad anordning för skapande av elektroniska stämplor som förvaltas av en kvalificerad tillhandahållare av betrodda tjänster i enlighet med artikel 39a för stämpelskaparens räkning.”
- h) Led 38 ska ersättas med följande:
- ”38. *certifikat för autentisering av webbplatser*: ett elektroniskt intyg som gör det möjligt att autentisera en webbplats och kopplar webbplatsen till den fysiska eller juridiska person som certifikatet utfärdats för.”
- i) Led 41 ska ersättas med följande:
- ”41. *validering*: en process genom vilken det kontrolleras och bekräftas att data i elektronisk form är giltiga i enlighet med denna förordning.”
- j) Följande led ska läggas till:
- ”42. *europeisk digital identitetsplånbok*: ett medel för elektronisk identifiering som gör det möjligt för användaren att på ett säkert sätt lagra, hantera och validera personidentitetsuppgifter och elektroniska attributsintyg i syfte att tillhandahålla dem till förlitande parter och andra användare av europeiska digitala identitetsplånböcker, och att underteckna med kvalificerade elektroniska underskrifter eller att stämpla med kvalificerade elektroniska stämplor.
43. *attribut*: en egenskap, en kvalitet, en rättighet eller ett tillstånd för en fysisk eller juridisk person eller ett föremål.
44. *elektroniskt attributsintyg*: ett intyg i elektronisk form som möjliggör autentisering av attribut.
45. *kvalificerat elektroniskt attributsintyg*: ett elektroniskt attributsintyg som är utfärdat av en kvalificerad tillhandahållare av betrodda tjänster och uppfyller kraven i bilaga V.
46. *elektroniskt attributsintyg utfärdat av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa*: ett elektroniskt attributsintyg utfärdat av ett offentligt organ som ansvarar för en autentisk källa eller av ett offentligt organ som utsetts av medlemsstaten för att utfärda sådana attributsintyg på uppdrag av de offentliga organ som ansvarar för autentiska källor i enlighet med artikel 45f och med bilaga VII.
47. *autentisk källa*: samlingsplats eller system, som innehas under ansvar av ett offentligt organ eller en privat enhet, som innehåller och tillhandahåller attribut om en fysisk eller juridisk person eller ett föremål och som anses vara en primärkälla för den informationen eller erkänns som autentisk i enlighet med unionsrätten eller nationell rätt, inbegripet administrativa förfaranden.

48. *elektronisk arkivering*: en tjänst som säkerställer mottagande, lagring, hämtning och radering av elektroniska uppgifter och elektroniska dokument i syfte att säkerställa deras hållbarhet och läsbarhet samt att bevara deras integritet, konfidentialitet och ursprungsbevis under hela bevarandeperioden.
 49. *kvalificerad elektronisk arkiveringstjänst*: en elektronisk arkiveringstjänst som tillhandahålls av en kvalificerad tillhandahållare av betrodda tjänster och som uppfyller de krav som fastställs i artikel 45j.
 50. *EU:s förtroendemärke för digitala identitetsplånböcker*: en kontrollerbar enkel och igenkännlig angivelse, visad på ett tydligt sätt, som meddelar att en europeisk digital identitetsplånbok har tillhandahållits i enlighet med denna förordning.
 51. *stark användarautentisering*: en autentisering som är baserad på användningen av åtminstone två autentiseringsfaktorer från olika kategorier av antingen kunskap (något som endast användaren känner till), besittning (något som endast användaren besitter) eller unik egenskap (något som användaren är) som är oberoende av varandra på ett sådant sätt att en incident avseende en av faktorerna inte äventyrar tillförlitligheten hos de andra, och som är utformad för att skydda konfidentialiteten för autentiseringsdata.
 52. *elektronisk liggare*: en sekvens av elektroniska dataloggar som säkerställer dataintegriteten och riktigheten i dessa loggars kronologiska ordning.
 53. *kvalificerad elektronisk liggare*: en elektronisk liggare som tillhandahålls av en kvalificerad tillhandahållare av betrodda tjänster och som uppfyller de krav som fastställs i artikel 45l.
 54. *personuppgifter*: varje upplysning enligt definitionen i artikel 4.1 i förordning (EU) 2016/679.
 55. *identitetsmatchning*: en process där uppgifter för personidentifiering eller medel för elektronisk identifiering matchas mot eller kopplas till ett befintligt konto som tillhör samma person.
 56. *datalogg*: elektroniska uppgifter som registrerats med tillhörande metadata som stöder behandlingen av dessa data.
 57. *offlineläge*: i fråga om användningen av europeiska digitala identitetsplånböcker, en interaktion mellan en användare och en tredje part på en fysisk plats med beröringsfri teknik, där det inte krävs att den europeiska digitala identitetsplånboken har åtkomst till system på distans via elektroniska kommunikationsnätverk för att genomföra interaktionen."
4. Artikel 5 ska ersättas med följande:

"Artikel 5

Pseudonymer vid elektroniska transaktioner

Utan att det påverkar tillämpningen av särskilda bestämmelser i unionsrätten eller nationell rätt som kräver att användarna ska identifiera sig, eller pseudonymers rättsverkan enligt nationell rätt, ska användning av pseudonymer valda av användaren inte vara förbjuden."

5. I kapitel II ska följande avsnitt införas:

"AVSNITT 1

EUROPEISK DIGITAL IDENTITETSPLÅNBOK

Artikel 5a

Europeiska digitala identitetsplånböcker

1. För att säkerställa att alla fysiska och juridiska personer i unionen har säker, tillitsbaserad och sömlös gränsöverskridande tillgång till offentliga och privata tjänster, samtidigt som de har full kontroll över sina uppgifter, ska varje medlemsstat tillhandahålla åtminstone en europeisk digital identitetsplånbok inom 24 månader från det att de genomförandeakter som avses i punkt 23 i denna artikel och i artikel 5c.6 träder i kraft.

2. Europeiska digitala identitetsplånböcker ska tillhandahållas på ett eller flera av följande sätt:
 - a) Direkt av en medlemsstat.
 - b) På uppdrag av en medlemsstat.
 - c) Oberoende av en medlemsstat men med den medlemsstatens erkännande.
3. Källkoden för programvarukomponenterna i europeiska digitala identitetsplånböcker ska vara licensierad med öppen källkod. Medlemsstaterna får föreskriva att källkoden för andra specifika komponenter än de som installeras på användarenheter inte ska lämnas ut om det föreligger vederbörligen motiverade skäl.
4. Europeiska digitala identitetsplånböcker ska göra det möjligt för användaren att, på ett sätt som är användarvänligt, transparent och spårbart för användaren,
 - a) på ett säkert sätt kunna begära, erhålla, välja, kombinera, lagra, radera, dela och visa, under användarens egen kontroll, uppgifter för personidentifiering och, i tillämpliga fall, i kombination med elektroniska attributsintyg, autentisera gentemot förlitande parter online och, i lämpliga fall, i offlineläge, i syfte att få tillgång till offentliga och privata tjänster, samtidigt som det säkerställs att selektivt utlämnande av data är möjligt,
 - b) generera pseudonymer och lagra dem i krypterad form lokalt i den europeiska digitala identitetsplånboken,
 - c) på ett säkert sätt autentisera en annan persons europeiska digitala identitetsplånbok och ta emot och dela uppgifter för personidentifierings och elektroniska attributsintyg på ett säkert sätt mellan de två europeiska digitala identitetsplånböckerna,
 - d) få tillgång till en logg över alla transaktioner som utförs genom den europeiska digitala identitetsplånboken via en gemensam instrumentpanel som gör det möjligt för användaren att
 - i) se en uppdaterad förteckning över förlitande parter med vilka användaren har upprättat en förbindelse och, i tillämpliga fall, alla utbytt uppgifter,
 - ii) på ett enkelt sätt begära att en förlitande part raderar personuppgifter enligt artikel 17 i förordning (EU) 2016/679,
 - iii) på ett enkelt sätt rapportera en förlitande part till den behöriga nationella dataskyddsmyndigheten, om en påstått olaglig eller misstänkt begäran om uppgifter tas emot,
 - e) underteckna med kvalificerade elektroniska underskrifter eller stämpla med kvalificerade elektroniska stämplor,
 - f) i den mån det är tekniskt möjligt ladda ned användarens uppgifter, elektroniska attributsintyg och konfigurationer,
 - g) utöva användarens rättigheter till dataportabilitet.
5. Europeiska digitala identitetsplånböcker ska i synnerhet
 - a) stödja gemensamma protokoll och gränssnitt
 - i) för utfärdande av uppgifter för personidentifiering, kvalificerade och icke-kvalificerade elektroniska attributsintyg eller kvalificerade och icke-kvalificerade certifikat till den europeiska digitala identitetsplånboken,
 - ii) för att förlitande parter ska kunna begära och validera uppgifter för personidentifiering och elektroniska attributsintyg,
 - iii) för delning och visning av uppgifter för personidentifiering, elektroniska attributsintyg eller selektivt utlämnade relaterade uppgifter för förlitande parter online och, när så är lämpligt, i offlineläge,

- iv) för att användaren ska kunna tillåta interaktion med den europeiska digitala identitetsplånboken och visa upp EU:s förtroendemärke för digitala identitetsplånböcker,
 - v) för säker anslutning av användaren genom användning av ett medel för elektronisk identifiering i enlighet med artikel 5a.24,
 - vi) för interaktion mellan två personers europeiska digitala identitetsplånböcker i syfte att ta emot, validera och dela uppgifter för personidentifiering och elektroniska attributsintyg på ett säkert sätt,
 - vii) för autentisering och identifiering av förlitande parter genom att autentiseringsmekanismer genomförs i enlighet med artikel 5b,
 - viii) för att förlitande parter ska kunna kontrollera europeiska digitala identitetsplånböckers äkthet och giltighet,
 - ix) för att begära att en förlitande part raderar personuppgifter enligt artikel 17 i förordning (EU) 2016/679,
 - x) för rapportering av en förlitande part till den behöriga nationella dataskyddsmyndigheten i fall då en påstått olaglig eller misstänkt begäran om data tas emot,
 - xi) för skapande av kvalificerade elektroniska underskrifter eller elektroniska stämplars genom anordningar för skapande av kvalificerade elektroniska underskrifter eller elektroniska stämplars,
- b) inte ge någon information till tillhandahållare av betrodda tjänster som tillhandahåller elektroniska attributsintyg om användningen av dessa elektroniska intyg,
- c) säkerställa att förlitande parter kan autentiseras och identifieras genom att autentiseringsmekanismer genomförs i enlighet med artikel 5b,
- d) uppfylla de krav som fastställs i artikel 8 vad gäller tillitnivå hög, särskilt när den tillämpas på kraven för styrkande och kontroll av identitet, och förvaltning och autentisering av medel för elektronisk identifiering,
- e) införa, i fråga om elektroniska attributsintyg med inbyggda policyer för utlämnande, en lämplig mekanism för att informera användaren om att den förlitande parten eller den användare av den europeiska digitala identitetsplånboken som begär det elektroniska attributsintyget har tillstånd att få tillgång till intyget,
- f) säkerställa att de uppgifter för personidentifiering som är tillgängliga från det system för elektronisk identifiering under vilket den europeiska digitala identitetsplånboken tillhandahålls, på ett unikt sätt avser den fysiska personen, den juridiska personen eller den fysiska person som företräder den fysiska eller juridiska personen, och är kopplade till den europeiska digitala identitetsplånboken,
- g) ge alla fysiska personer möjlighet att som utgångspunkt och kostnadsfritt underteckna med kvalificerade elektroniska underskrifter.

Trots första stycket g får medlemsstaterna föreskriva proportionella åtgärder för att säkerställa att fysiska personers kostnadsfria användning av kvalificerade elektroniska underskrifter är begränsad till icke-yrkesmässiga ändamål.

6. Medlemsstaterna ska utan dröjsmål informera användare om eventuella säkerhetsincidenter som helt eller delvis kan ha äventyrat deras europeiska digitala identitetsplånbok eller dess innehåll, särskilt om deras europeiska digitala identitetsplånbok har upphävts tillfälligt eller återkallats enligt artikel 5e,

7. Utan att det påverkar tillämpningen av artikel 5f får medlemsstaterna, i enlighet med nationell rätt, föreskriva ytterligare funktioner för europeiska digitala identitetsplånböcker, inbegripet interoperabilitet med befintliga nationella medel för elektronisk identifiering. Dessa ytterligare funktioner ska överensstämma med den här artikeln.

8. Medlemsstaterna ska tillhandahålla valideringsmekanismer kostnadsfritt i syfte att
 - a) säkerställa att europeiska digitala identitetsplånböckers äkthet och giltighet kan kontrolleras,
 - b) göra det möjligt för användare att kontrollera äkthet och giltighet för identiteten hos de förlitande parter som registrerats i enlighet med artikel 5b.
9. Medlemsstaterna ska säkerställa att den europeiska digitala identitetsplånbokens giltighet kan återkallas
 - a) på användarens uttryckliga begäran,
 - b) när den europeiska digitala identitetsplånbokens säkerhet har äventyrats,
 - c) vid användarens död eller när den juridiska personen upphör med sin verksamhet.
10. Tillhandahållare av europeiska digitala identitetsplånböcker ska säkerställa att användarna enkelt kan begära tekniskt stöd och rapportera tekniska problem eller andra incidenter som har en negativ inverkan på användningen av europeiska digitala identitetsplånböcker.
11. Europeiska digitala identitetsplånböcker ska tillhandahållas enligt ett system för elektronisk identifiering med tillitsnivå hög.
12. Europeiska digitala identitetsplånböcker ska säkerställa inbyggd säkerhet.
13. Utfärdandet, användningen och återkallandet av europeiska digitala identitetsplånböcker ska vara utan kostnad för alla fysiska personer.
14. Användarna ska ha full kontroll över användningen av, och uppgifterna i, sin europeiska digitala identitetsplånbok. Tillhandahållaren av den europeiska digitala identitetsplånboken får varken samla in sådan information om användningen av den europeiska digitala identitetsplånboken som inte är nödvändig för tillhandahållandet av tjänster relaterade till den europeiska digitala identitetsplånboken eller kombinera uppgifter för personidentifiering eller några andra personuppgifter som lagras eller som rör användningen av den europeiska digitala identitetsplånboken med personuppgifter från andra tjänster som erbjuds av den tillhandahållaren eller från tredjepartstjänster och som inte krävs för tillhandahållandet av tjänster relaterade till den europeiska digitala identitetsplånboken, om inte användaren uttryckligen har begärt detta. Personuppgifter som rör tillhandahållandet av den europeiska digitala identitetsplånboken ska hållas logiskt avskilda från andra data som innehas av tillhandahållaren av europeiska digitala identitetsplånböcker. Om den europeiska digitala identitetsplånboken tillhandahålls av privata parter i enlighet med punkt 2 b och c i denna artikel, ska bestämmelserna i artikel 45h.3 gälla i tillämpliga delar.
15. Användningen av europeiska digitala identitetsplånböcker ska vara frivillig. Tillgången till offentliga och privata tjänster, tillträdet till arbetsmarknaden och näringsfriheten får inte på något sätt begränsas eller göras ofördelaktiga för fysiska eller juridiska personer som inte använder europeiska digitala identitetsplånböcker. Det ska alltjämt vara möjligt att få tillgång till offentliga och privata tjänster med hjälp av andra befintliga medel för identifiering och autentisering.
16. Det tekniska ramverket för den europeiska digitala identitetsplånboken ska
 - a) inte tillåta tillhandahållare av elektroniska attributsintyg eller någon annan part att, efter utfärdandet av attributsintyget, erhålla data som gör det möjligt att spåra, länka, korrelera transaktioner eller användarbeteende eller på annat sätt få kännedom om transaktioner eller användarbeteende, såvida inte användaren uttryckligen har gett sitt tillstånd till detta,
 - b) möjliggöra integritetsbevarande teknik som säkerställer att länkning är omöjlig, om attributsintyget inte kräver identifiering av användaren.
17. All behandling av personuppgifter som utförs av medlemsstaterna eller på deras vägnar av organ eller parter som ansvarar för tillhandahållandet av europeiska digitala identitetsplånböcker som medel för elektronisk identifiering ska utföras i enlighet med lämpliga och effektiva dataskyddsåtgärder. Behandlingens förenlighet med förordning (EU) 2016/679 ska visas. Medlemsstaterna får införa nationella bestämmelser för att ytterligare specificera tillämpningen av sådana åtgärder.

18. Medlemsstaterna ska utan onödigt dröjsmål informera kommissionen om
- det organ som ansvarar för att upprätta och underhålla förteckningen över registrerade förlitande parter som förlitar sig på de europeiska digitala identitetsplånböckerna i enlighet med artikel 5b.5 och var den förteckningen finns tillgänglig,
 - de organ som ansvarar för tillhandahållandet av de europeiska digitala identitetsplånböckerna i enlighet med artikel 5a.1,
 - de organ som ansvarar för att säkerställa att uppgifterna för personidentifiering är kopplade till den europeiska digitala identitetsplånboken i enlighet med artikel 5a.5 f,
 - den mekanism som gör det möjligt att validera de uppgifter för personidentifiering som avses i artikel 5a.5 f och de förlitande parternas identitet,
 - mekanismen för validering av de europeiska digitala identitetsplånböckernas äkthet och giltighet.

Kommissionen ska göra den information som avses i första stycket tillgänglig för allmänheten genom en säker kanal i elektroniskt undertecknad eller stämplad form som lämpar sig för automatiserad behandling.

19. Utan att det påverkar tillämpningen av punkt 22 i denna artikel ska artikel 11 i tillämpliga delar gälla för den europeiska digitala identitetsplånboken.

20. Artikel 24.2 b och d–h ska gälla i tillämpliga delar för tillhandahållare av europeiska digitala identitetsplånböcker.

21. Europeiska digitala identitetsplånböcker ska göras tillgängliga för användning av personer med funktionsnedsättning, på samma villkor som andra användare, i enlighet med Europaparlamentets och rådets direktiv (EU) 2019/882 (*).

22. Vid tillhandahållandet av europeiska digitala identitetsplånböcker ska de europeiska digitala identitetsplånböckerna och de system för elektronisk identifiering inom ramen för vilka de tillhandahålls inte omfattas av de krav som fastställs i artiklarna 7, 9, 10, 12 och 12a.

23. Senast den 21 november 2024 ska kommissionen, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för de krav som avses i punkterna 4, 5, 8 och 18 i denna artikel om genomförandet av den europeiska digitala identitetsplånboken. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

24. Kommissionen ska genom genomförandeakter upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för att främja anslutning av användare till den europeiska digitala identitetsplånboken, antingen genom medel för elektronisk identifiering som motsvarar tillitsnivå hög eller medel för elektronisk identifiering som motsvarar tillitsnivå väsentlig i kombination med ytterligare förfaranden för anslutning på distans som tillsammans uppfyller kraven för tillitsnivå hög. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 5b

Europeiska digitala identitetsplånboken – förlitande parter

1. Om en förlitande part avser att förlita sig på europeiska digitala identitetsplånböcker för tillhandahållande av offentliga eller privata tjänster genom digital interaktion ska den förlitande parten registrera sig i den medlemsstat där den är etablerad.

2. Registreringsprocessen ska vara kostnadseffektiv och stå i proportion till riskerna. Den förlitande parten ska tillhandahålla åtminstone följande:

- Den information som krävs för autentisering till europeiska digitala identitetsplånböcker, som omfattar minst
 - den medlemsstat där den förlitande parten är etablerad, och

- ii) den förlitande partens namn och, i tillämpliga fall, dess registreringsnummer i enlighet med vad som framgår i ett officiellt register, tillsammans med identifieringsuppgifter från det officiella registret.
- b) Kontaktuppgifter till den förlitande parten.
- c) Den avsedda användningen av europeiska digitala identitetsplånböcker, inbegripet angivande av de uppgifter som den förlitande parten ska begära från användare.
3. Förlitande parter får inte begära att användare tillhandahåller några andra uppgifter än dem som anges enligt punkt 2 c.
4. Punkterna 1 och 2 ska inte påverka tillämpningen av unionsrätt eller nationell rätt som är tillämplig på tillhandahållandet av särskilda tjänster.
5. Medlemsstaterna ska göra den information som avses i punkt 2 tillgänglig för allmänheten online i elektronisk undertecknad eller stämplad form som lämpar sig för automatiserad behandling.
6. Förlitande parter som registrerat sig i enlighet med denna artikel ska utan dröjsmål informera medlemsstaterna om eventuella ändringar av den information som lämnats vid registreringen enligt punkt 2.
7. Medlemsstaterna ska tillhandahålla en gemensam mekanism för att möjliggöra identifiering och autentisering av förlitande parter, enligt vad som avses i artikel 5a.5 c.
8. Om förlitande parter avser att förlita sig på europeiska digitala identitetsplånböcker ska de identifiera sig för användaren.
9. Förlitande parter ska ansvara för genomförandet av förfarandet för autentisering och validering av uppgifter för personidentifiering och elektroniska attributsintyg som begärts från europeiska digitala identitetsplånböcker. Förlitande parter får inte neka användning av pseudonymer om identifiering av användaren inte krävs enligt unionsrätten eller nationell rätt.
10. Mellanhänder som agerar för förlitande parters räkning ska betraktas som förlitande parter och får inte lagra uppgifter om transaktionens innehåll.
11. Senast den 21 november 2024 ska kommissionen fastställa tekniska specifikationer och förfaranden för de krav som avses i punkterna 2, 5 och 6-9 i denna artikel genom genomförandeakter om det genomförande av europeiska digitala identitetsplånböcker som avses i artikel 5a.23. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 5c

Certifiering av europeiska digitala identitetsplånböcker

1. Certifiering av att europeiska digitala identitetsplånböcker och de system för elektronisk identifiering inom ramen för vilka de tillhandahålls överensstämmer med kraven i artikel 5a.4, 5a.5 och 5a.8, kravet på logiskt avskiljande i artikel 5a.14 och, i tillämpliga fall, de standarder och tekniska specifikationer som avses i artikel 5a.24 ska utföras av organ för bedömning av överensstämmelse som utsetts av medlemsstaterna.
2. Certifiering av att europeiska digitala identitetsplånböcker överensstämmer med de krav som avses i punkt 1 i denna artikel, eller delar av dem, som är relevanta för cybersäkerhet ska utföras i enlighet med europeiska cybersäkerhetscertifieringsordningar som antagits enligt Europaparlamentets och rådets förordning (EU) 2019/881 (***) och som avses i de genomförandeakter som avses i punkt 6 i denna artikel.
3. För krav som avses i punkt 1 i denna artikel som inte är relevanta för cybersäkerhet och för krav som avses i punkt 1 i denna artikel som är relevanta för cybersäkerhet, i den mån som de ordningar för cybersäkerhetscertifiering som avses i punkt 2 i denna artikel inte, eller endast delvis, omfattar de cybersäkerhetskraven, ska medlemsstaterna även för de kraven inrätta nationella certifieringsordningar i enlighet med de krav som fastställs i de genomförandeakter som avses i punkt 6 i denna artikel. Medlemsstaterna ska översända sina utkast till nationella certifieringsordningar till den europeiska samarbetsgrupp för digital identitet som inrättats enligt artikel 46e.1 (samarbetsgruppen). Samarbetsgruppen får utfärda yttranden och rekommendationer.

4. Certifiering enligt punkt 1 ska vara giltig i upp till fem år, under förutsättning att en sårbarhetsbedömning utförs vartannat år. Om en sårbarhet identifieras och inte åtgärdas inom lämplig tid, ska certifieringen upphöra att gälla.
5. Överensstämmelse med kraven i artikel 5a i denna förordning avseende behandling av personuppgifter får certifieras enligt förordning (EU) 2016/679.
6. Senast den 21 november 2024 ska kommissionen, genom genomförandeakter, upprätta en förteckning över referensstandarder och vid behov fastställa specifikationer och förfaranden för certifiering av europeiska digitala identitetsplånböcker som avses i punkterna 1, 2 och 3 i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.
7. Medlemsstaterna ska meddela kommissionen namn och adress för de organ för bedömning av överensstämmelse som avses i punkt 1. Kommissionen ska göra den informationen tillgänglig för samtliga medlemsstater.
8. Kommissionen ska ha befogenhet att anta delegerade akter i enlighet med artikel 47 om fastställande av särskilda kriterier som ska uppfyllas av de utsedda organ för bedömning av överensstämmelse som avses i punkt 1 i den här artikeln.

Artikel 5d

Offentliggörande av en förteckning över certifierade europeiska digitala identitetsplånböcker

1. Medlemsstaterna ska utan onödigt dröjsmål informera kommissionen och den samarbetsgrupp som inrättats i enlighet med artikel 46e.1 om europeiska digitala identitetsplånböcker som har tillhandahållits i enlighet med artikel 5a och som har certifierats av de organ för bedömning av överensstämmelse som avses i artikel 5c.1. De ska utan onödigt dröjsmål informera kommissionen och den samarbetsgrupp som inrättats i enlighet med artikel 46e.1 om en certifiering upphör att gälla och ange skälen till detta.
2. Utan att det påverkar tillämpningen av artikel 5a.18 ska den information som medlemsstaterna lämnar enligt punkt 1 i den här artikeln åtminstone omfatta uppgifter om följande:
 - a) Certifikatet och rapporten om certifieringsbedömningen för den certifierade europeiska digitala identitetsplånboken.
 - b) En beskrivning av det system för elektronisk identifiering inom ramen för vilket den europeiska digitala identitetsplånboken tillhandahålls.
 - c) Det tillämpliga tillsynssystemet samt information om systemet för skadeståndsansvar med avseende på den part som tillhandahåller den europeiska digitala identitetsplånboken.
 - d) Den myndighet eller de myndigheter som ansvarar för systemet för elektronisk identifiering.
 - e) System för tillfälligt upphävande eller återkallande av det anmälda systemet för elektronisk identifiering eller autentisering eller av de berörda äventytrade delarna.
3. Kommissionen ska på grundval av den information som inkommit i enlighet med punkt 1 upprätta, offentliggöra i *Europeiska unionens officiella tidning* och i maskinläsbar form upprätthålla en förteckning över certifierade europeiska digitala identitetsplånböcker.
4. En medlemsstat får lämna in en begäran till kommissionen om att ta bort en europeisk digital identitetsplånbok och det system för elektronisk identifiering inom ramen för vilket den tillhandahålls från den förteckning som avses i punkt 3.
5. Om den information som lämnats i enlighet med punkt 1 ändras ska medlemsstaten förse kommissionen med uppdaterad information.
6. Kommissionen ska hålla den förteckning som avses i punkt 3 uppdaterad genom att i *Europeiska unionens officiella tidning* offentliggöra motsvarande ändringar av förteckningen inom en månad från mottagandet av en begäran enligt punkt 4 eller av uppdaterad information enligt punkt 5.

7. Senast den 21 november 2024 ska kommissionen fastställa de format och förfaranden som ska gälla vid tillämpning av punkterna 1, 4 och 5 i denna artikel; detta ska göras genom genomförandeakter om genomförandet av europeiska digitala identitetsplånböcker som avses i artikel 5a.23. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 5e

Säkerhetsincidenter som rör europeiska digitala identitetsplånböcker

1. I de fall då europeiska digitala identitetsplånböcker som tillhandahålls i enlighet med artikel 5a, de valideringsmekanismer som avses i artikel 5a.8 eller det system för elektronisk identifiering inom ramen för vilket de europeiska digitala identitetsplånböckerna tillhandahålls är föremål för incidenter eller delvis äventyras på ett sätt som påverkar deras tillförlitlighet, eller tillförlitligheten för andra europeiska digitala identitetsplånböcker, ska den medlemsstat som tillhandahåller de europeiska digitala identitetsplånböckerna utan onödigt dröjsmål tillfälligt upphäva tillhandahållandet och användningen av europeiska digitala identitetsplånböcker.

När det är motiverat mot bakgrund av allvaret i den säkerhetsincident eller det äventyrande som avses i första stycket ska medlemsstaten återkalla europeiska digitala identitetsplånböcker utan onödigt dröjsmål.

Medlemsstaten ska informera de berörda användarna, de gemensamma kontaktpunkter som utsetts i enlighet med artikel 46c.1, de förlitande parterna och kommissionen om detta.

2. Om den säkerhetsincident eller det äventyrande som avses i punkt 1 första stycket i denna artikel inte åtgärdas inom tre månader från det tillfälliga upphävandet, ska den medlemsstat som tillhandahåller de europeiska digitala identitetsplånböckerna återkalla europeiska digitala identitetsplånböckerna och upphäva deras giltighet. Medlemsstaten ska informera de berörda användarna, de gemensamma kontaktpunkter som utsetts i enlighet med artikel 46c.1, de förlitande parterna och kommissionen om återkallandet.

3. I fall då den säkerhetsincident eller det äventyrande som avses i punkt 1 första stycket i denna artikel åtgärdas ska den tillhandahållande medlemsstaten återupprätta tillhandahållandet och användningen av europeiska digitala identitetsplånböcker och informera de berörda användarna och förlitande parterna samt de gemensamma kontaktpunkter som utsetts i enlighet med artikel 46c.1 och kommissionen utan onödigt dröjsmål.

4. Kommissionen ska utan onödigt dröjsmål offentliggöra motsvarande ändringar i den förteckning som avses i artikel 5d i *Europeiska unionens officiella tidning*.

5. Senast den 21 november 2024 ska kommissionen, genom genomförandeakter, fastställa en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för de åtgärder som avses i punkterna 1, 2 och 3 i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 5f

Gränsöverskridande användning av europeiska digitala identitetsplånböcker

1. I de fall då medlemsstater kräver elektronisk identifiering och autentisering för att få åtkomst till en nättjänst som tillhandahålls av ett offentligt organ, ska de även godta europeiska digitala identitetsplånböcker som tillhandahålls i enlighet med denna förordning.

2. I de fall då privata förlitande parter som tillhandahåller tjänster, med undantag för mikroföretag och små företag enligt definitionen i artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG (***) enligt unionsrätten eller nationell rätt är ålagda att använda stark användarautentisering för onlineidentifiering, eller om stark användarautentisering för onlineidentifiering krävs enligt avtalsförpliktelse, inbegripet på områdena transport, energi, banktjänster, finansiella tjänster, social trygghet, hälso- och sjukvård, dricksvatten, posttjänster, digital infrastruktur, utbildning eller telekommunikation, ska dessa privata förlitande parter senast 36 månader efter dagen för ikraftträdandet av de genomförandeakter som avses i artiklarna 5a.23 och 5c.6, och endast på användarens frivilliga begäran, även godta europeiska digitala identitetsplånböcker som tillhandahålls i enlighet med denna förordning.

3. I de fall då tillhandahållare av mycket stora onlineplattformar enligt artikel 33 i Europaparlamentets och rådets förordning (EU) 2022/2065 (***) kräver användarautentisering för att få åtkomst till nättjänster, ska dessa plattformar även godta och främja användningen av europeiska digitala identitetsplånböcker som tillhandahålls i enlighet med denna förordning när det gäller användarautentisering endast på användarens frivilliga begäran och iaktta de minimidata som behövs för den specifika nättjänst som begäran om autentisering avser.
4. I samarbete med medlemsstaterna ska kommissionen främja utvecklingen av uppförandekoder i nära samarbete med berörda parter, inbegripet civilsamhället, för att bidra till en bred tillgång till och användbarhet för europeiska digitala identitetsplånböcker inom ramen för denna förordning, och för att uppmuntra tjänsteleverantörer att slutföra utarbetandet av uppförandekoder.
5. Inom 24 månader från införandet av europeiska digitala identitetsplånböcker ska kommissionen bedöma efterfrågan på, och tillgången till, europeiska digitala identitetsplånböcker samt deras användbarhet, med beaktande av kriterier såsom spridning bland användarna, tjänsteleverantörers gränsöverskridande närvaro, teknisk utveckling, användningsmönstrens utveckling och konsumenternas efterfrågan.
- (*) Europaparlamentets och rådets direktiv (EU) 2019/882 av den 17 april 2019 om tillgänglighetskrav för produkter och tjänster (EUT L 151, 7.6.2019, s. 70).
- (**) Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten) (EUT L 151, 7.6.2019, s. 15).
- (***) Kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag (EUT L 124, 20.5.2003, s. 36).
- (****) Europaparlamentets och rådets förordning (EU) 2022/2065 av den 19 oktober 2022 om en inre marknad för digitala tjänster och om ändring av direktiv 2000/31/EG (förordningen om digitala tjänster) (EUT L 277, 27.10.2022, s. 1)."

6. Följande rubrik ska införas före artikel 6:

"AVSNITT 2

SYSTEM FÖR ELEKTRONISK IDENTIFIERING"

7. I artikel 7 ska led g ersättas med följande:

"g) Minst sex månader före anmälan enligt artikel 9.1 ska den anmälande medlemsstaten för tillämpningen av artikel 12.5 förse andra medlemsstater med en beskrivning av detta system i enlighet med de förfaranden som fastställts genom de genomförandeakter som antas enligt artikel 12.6."

8. I artikel 8.3 ska första stycket ersättas med följande:

"3. Senast den 18 september 2015 ska kommissionen, med beaktande av relevanta internationella standarder och om inte annat följer av punkt 2, genom genomförandeakter fastställa tekniska minimispecifikationer, standarder och förfaranden genom vilka tillitsnivåerna låg, väsentlig och hög specificeras för medel för elektronisk identifiering."

9. Artikel 9.2 och 9.3 ska ersättas med följande:

"2. Kommissionen ska utan onödigt dröjsmål i *Europeiska unionens officiella tidning* offentliggöra en förteckning över de system för elektronisk identifiering som anmälts enligt punkt 1 tillsammans med de grundläggande uppgifterna om dessa system.

3. Kommissionen ska i *Europeiska unionens officiella tidning* offentliggöra ändringarna i den förteckning som avses i punkt 2 inom en månad från den dag då anmälan mottogs."

10. I artikel 10 ska rubriken ersättas med följande:

"Säkerhetsincidenter som rör system för elektronisk identifiering".

11. Följande artikel ska införas:

"Artikel 11a

Gränsöverskridande identitetsmatchning

1. När medlemsstater agerar som förlitande parter för gränsöverskridande tjänster ska de säkerställa otvetydig identitetsmatchning för fysiska personer som använder anmälda medel för elektronisk identifiering eller europeiska digitala identitetsplånböcker.

2. Medlemsstaterna ska föreskriva tekniska och organisatoriska åtgärder för att säkerställa en hög skyddsnivå för personuppgifter som används för identitetsmatchning och för att förhindra profilering av användare.

3. Senast den 21 november 2024 ska kommissionen, genom genomförandeakter, fastställa en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för de krav som avses i punkt 1 i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2."

12. Artikel 12 ska ändras på följande sätt:

a) Rubriken ska ersättas med följande:

"Interoperabilitet".

b) Punkt 3 ska ändras på följande sätt:

i) Led c ska ersättas med följande:

"c) Det ska främja genomförandet av inbyggt integritetsskydd och inbyggt säkerhet."

ii) Led d ska utgå.

c) I punkt 4 ska led d ersättas med följande:

"d) Hänvisning till en minimuppsättning uppgifter för personidentifiering som krävs för att på ett unikt sätt avse en fysisk eller juridisk person eller en fysisk person som företräder en annan fysisk person eller en juridisk person och som är tillgänglig via system för elektronisk identifiering."

d) Punkterna 5 och 6 ska ersättas med följande:

"5. Medlemsstaterna ska genomföra sakkunnigbedömningar av de system för elektronisk identifiering som omfattas av tillämpningsområdet för denna förordning och som ska anmälas enligt artikel 9.1 a.

6. Senast den 18 mars 2025 ska kommissionen genom genomförandeakter fastställa nödvändiga förfaranden för de sakkunnigbedömningar som avses i punkt 5 i denna artikel i syfte att främja en hög nivå av förtroende och säkerhet som står i proportion till risknivån. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2."

e) Punkt 7 ska utgå.

f) Punkt 8 ska ersättas med följande:

"8. Senast den 18 september 2025 ska kommissionen, för att fastställa enhetliga villkor för tillämpningen av kraven i punkt 1 i denna artikel, i enlighet med de kriterier som fastställs i punkt 3 i denna artikel och med beaktande av resultaten av samarbetet mellan medlemsstaterna, anta genomförandeakter om det interoperabilitetsramverk som anges i punkt 4 i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2."

13. Följande artiklar ska införas i kapitel II:

Artikel 12a

Certifiering av system för elektronisk identifiering

1. Överensstämmelse för system för elektronisk identifiering som ska anmälas med de cybersäkerhetskrav som fastställs i denna förordning, inbegripet överensstämmelse med de relevanta cybersäkerhetskrav som fastställs i artikel 8.2 vad gäller tillitsnivåerna för system för elektronisk identifiering, ska certifieras av organ för bedömning av överensstämmelse som utsetts av medlemsstaterna.
2. Den certifiering enligt punkt 1 i denna artikel ska utföras inom ramen för en relevant ordning för cybersäkerhetscertifiering enligt förordning (EU) 2019/881 eller delar därav, i den mån cybersäkerhetscertifikatet eller delar därav omfattar dessa cybersäkerhetskrav.
3. Certifiering i enlighet med punkt 1 ska gälla i upp till fem år, under förutsättning att en sårbarhetsbedömning genomförs vartannat år. Om en sårbarhet identifieras och inte åtgärdas inom tre månader från identifieringen, ska certifieringen upphöra att gälla.
4. Trots vad som sägs i punkt 2 får medlemsstaterna, i enlighet med den punkten, begära ytterligare information från en anmälade medlemsstat om system för elektronisk identifiering eller delar därav som certifieras.
5. Den sakkunnigbedömning av system för elektronisk identifiering som avses i artikel 12.5 ska inte tillämpas på de system för elektronisk identifiering, eller delar av sådana system, som certifierats i enlighet med punkt 1 i den här artikeln. Medlemsstaterna får använda ett certifikat eller en försäkran om överensstämmelse, som utfärdats i enlighet med en relevant europeisk ordning för cybersäkerhetscertifiering eller delar av en sådan ordning, när det gäller krav som inte avser cybersäkerhet enligt artikel 8.2 avseende tillitsnivån för system för elektronisk identifiering.
6. Medlemsstaterna ska meddela kommissionen namn och adress för de organ för bedömning av överensstämmelse som avses i punkt 1. Kommissionen ska göra den informationen tillgänglig för samtliga medlemsstater.

Artikel 12b

Tillgång till maskinvaru- och programvarufunktioner

Om tillhandahållare av europeiska digitala identitetsplånböcker och utfärdare av anmälda medel för elektronisk identifiering som agerar kommersiellt eller yrkesmässigt och använder centrala plattformstjänster enligt definitionen i artikel 2.2 i Europaparlamentets och rådets förordning (EU) 2022/1925 (*) för eller i samband med tillhandahållande av tjänster relaterade till europeiska digitala identitetsplånböcker och medel för elektronisk identifiering till slutanvändare är företagsanvändare i enlighet med artikel 2.21 i den förordningen, ska grindvakter särskilt tillåta dem faktisk interoperabilitet med och, för interoperabilitetsändamål, åtkomst till samma operativsystem eller maskinvaru- eller programvarufunktioner. Sådan faktisk interoperabilitet och åtkomst ska tillåtas kostnadsfritt och oavsett om maskinvaru- eller programvarufunktionerna är en del av det operativsystem som grindvakter har tillgång till eller använder när denne tillhandahåller sådana tjänster, i den mening som avses i artikel 6.7 i förordning (EU) 2022/1925. Den här artikeln påverkar inte tillämpningen av artikel 5a.14 i den här förordningen.

(*) Europaparlamentets och rådets förordning (EU) 2022/1925 av den 14 september 2022 om öppna och rättvisa marknader inom den digitala sektorn och om ändring av direktiv (EU) 2019/1937 och (EU) 2020/1828 (förordningen om digitala marknader) (EUT L 265, 12.10.2022, s. 1)."

14. Artikel 13.1 ska ersättas med följande:

"1. Trots punkt 2 i denna artikel och utan att det påverkar tillämpningen av förordning (EU) 2016/679 ska tillhandahållare av betrodda tjänster ha skadeståndsansvar för skada som åsamkats en fysisk eller juridisk person avsiktligt eller på grund av oaktsamhet genom deras underlåtenhet att uppfylla sina skyldigheter enligt denna förordning. Varje fysisk eller juridisk person som har lidit materiell eller immateriell skada till följd av en överträdelse av denna förordning av en tillhandahållare av betrodda tjänster ska ha rätt att begära ersättning i enlighet med unionsrätten och nationell rätt.

Bevisbördan för avsikt eller oaktsamhet hos en icke-kvalificerad tillhandahållare av betrodda tjänster ska vila på den fysiska eller juridiska person som gör gällande sådan skada som avses i första stycket.

Avsikt eller oaktsamhet hos en kvalificerad tillhandahållare av betrodda tjänster med avseende på skada som avses i första stycket ska presumeras såvida inte den kvalificerade tillhandahållaren av betrodda tjänster bevisar att den skada som avses i första stycket har uppstått utan avsikt eller oaktsamhet hos den kvalificerade tillhandahållaren av betrodda tjänster."

15. Artiklarna 14, 15 och 16 ska ersättas med följande:

"Artikel 14

Internationella aspekter

1. Betrodda tjänster som tillhandahålls av tillhandahållare av betrodda tjänster som är etablerade i ett tredjeland eller av en internationell organisation ska erkännas som rättsligt likvärdiga med kvalificerade betrodda tjänster som tillhandahålls av kvalificerade tillhandahållare av betrodda tjänster som är etablerade inom unionen, under förutsättning att de betrodda tjänsterna från tredjelandet eller från den internationella organisationen är erkända genom genomförandeakter eller ett avtal som ingåtts mellan unionen och tredjelandet eller den internationella organisationen enligt artikel 218 i EUF-fördraget.

De genomförandeakter som avses i första stycket ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

2. De genomförandeakter och det avtal som avses i punkt 1 ska säkerställa att de krav som är tillämpliga på kvalificerade tillhandahållare av betrodda tjänster som är etablerade inom unionen och de kvalificerade betrodda tjänster som de tillhandahåller uppfylls av tillhandahållarna av betrodda tjänster i det berörda tredjelandet eller av den internationella organisationen och av de betrodda tjänster som de tillhandahåller. Tredjeländer och internationella organisationer ska särskilt upprätta, underhålla och offentliggöra en förteckning över erkända tillhandahållare av betrodda tjänster.

3. De avtal som avses i punkt 1 ska säkerställa att de kvalificerade betrodda tjänster som tillhandahålls av kvalificerade tillhandahållare av betrodda tjänster som är etablerade inom unionen erkänns som rättsligt likvärdiga med betrodda tjänster som tillhandahålls av tillhandahållare av betrodda tjänster i det tredjeland eller av den internationella organisation med vilket eller vilken avtalet ingås.

Artikel 15

Tillgänglighet för personer med funktionsnedsättning och särskilda behov

Tillhandahållandet av medel för elektronisk identifiering, betrodda tjänster och slutanvändarprodukter som används vid tillhandahållandet av dessa tjänster ska göras tillgängliga på ett klart och begripligt språk, i enlighet med Förenta nationernas konvention om rättigheter för personer med funktionsnedsättning och med tillgänglighetskraven i direktiv (EU) 2019/882, och därmed även gynna personer med funktionsbegränsningar, såsom äldre personer, och personer med begränsad tillgång till digital teknik."

Artikel 16

Sanktioner

1. Utan att det påverkar tillämpningen av artikel 31 i Europaparlamentets och rådets direktiv (EU) 2022/2555 (*) ska medlemsstaterna fastställa bestämmelser om sanktioner som ska gälla vid överträdelser av denna förordning. Sanktionerna ska vara effektiva, proportionella och avskräckande.

2. Medlemsstaterna ska säkerställa att överträdelser av denna förordning som begås av kvalificerade och icke-kvalificerade tillhandahållare av betrodda tjänster medför maximala administrativa sanktionsavgifter på minst

a) 5 000 000 EUR om tillhandahållaren av betrodda tjänster är en fysisk person, eller

b) om tillhandahållaren av betrodda tjänster är en juridisk person, 5 000 000 EUR eller 1 % av den totala globala årsomsättningen för det företag som tillhandahållaren av betrodda tjänster tillhörde under det räkenskapsår som föregick det år då överträdelsen inträffade, beroende på vilket som är högst.

3. Beroende på medlemsstaternas rättssystem får reglerna om administrativa sanktionsavgifter tillämpas på ett sådant sätt att förfarandet inleds av det behöriga tillsynsorganet och sanktionsavgifterna påförs av behöriga nationella domstolar. Tillämpningen av sådana regler i dessa medlemsstater ska säkerställa att dessa rättsmedel är effektiva och har motsvarande verkan som de administrativa sanktionsavgifter som påförs direkt av tillsynsmyndigheter.

(*) Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972, och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet) (EUT L 333, 27.12.2022, s. 80)."

16. I kapitel III avsnitt 2 ska titeln ersättas med följande:

"Icke-kvalificerade betrodda tjänster"

17. Artiklarna 17 och 18 ska utgå.

18. Följande artikel ska införas i kapitel III avsnitt 2:

"Artikel 19a

Krav på icke-kvalificerade tillhandahållare av betrodda tjänster

1. En icke-kvalificerad tillhandahållare av betrodda tjänster som tillhandahåller icke-kvalificerade betrodda tjänster ska

a) ha lämpliga policyer och vidta motsvarande åtgärder för att hantera rättsliga, affärsmässiga, operativa och andra direkta eller indirekta risker för tillhandahållandet av icke-kvalificerade betrodda tjänster, som trots artikel 21 i direktiv (EU) 2022/2555, ska innefatta åtminstone åtgärder avseende

- i) registrerings- och anslutningsförfaranden för en tjänst,
- ii) förfarandemässiga eller administrativa kontroller som krävs för att tillhandahålla betrodda tjänster,
- iii) förvaltning och genomförande av betrodda tjänster,

b) anmäla till tillsynsorganet, de identifierbara berörda personerna, allmänheten om det är av allmänt intresse och, om tillämpligt, andra relevanta behöriga myndigheter, alla säkerhetsincidenter eller störningar vid tillhandahållandet av tjänsten eller genomförandet av de åtgärder som avses i led a i, ii eller iii och som har en betydande inverkan på den tillhandahållna betrodda tjänsten eller de personuppgifter som lagras däri, utan onödigt dröjsmål och under alla omständigheter inom 24 timmar från säkerhetsincidenten eller störningen.

2. Senast den 21 maj 2025 ska kommissionen, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden avseende punkt 1 a i denna artikel. Överensstämmelse med kraven i denna artikel ska presumeras om dessa standarder, specifikationer och förfaranden uppfylls. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2."

19. Artikel 20 ska ändras på följande sätt:

a) Punkt 1 ska ersättas med följande:

"1. Kvalificerade tillhandahållare av betrodda tjänster ska minst en gång vartannat år och på egen bekostnad granskas av ett organ för bedömning av överensstämmelse. Granskningen ska bekräfta att de kvalificerade tillhandahållarna av betrodda tjänster och de kvalificerade betrodda tjänster som de tillhandahåller uppfyller kraven i denna förordning och i artikel 21 i direktiv (EU) 2022/2555. Kvalificerade tillhandahållare av betrodda tjänster ska lämna in den resulterande rapporten om bedömning av överensstämmelse till tillsynsorganet inom tre arbetsdagar från mottagandet."

b) Följande punkter ska införas:

"1a. Kvalificerade tillhandahållare av betrodda tjänster ska senast en månad före en planerad revision informera tillsynsorganet och ska tillåta tillsynsorganet att på begäran delta som observatör.

1b. Medlemsstaterna ska utan onödigt dröjsmål till kommissionen anmäla namn, adress och ackrediteringsuppgifter för de organ för bedömning av överensstämmelse som avses i punkt 1 och eventuella senare ändringar av dessa. Kommissionen ska göra den informationen tillgänglig för samtliga medlemsstater.”

c) Punkterna 2, 3 och 4 ska ersättas med följande:

”2. Tillsynsorganet får, utan att det påverkar tillämpningen av punkt 1, när som helst granska eller begära att ett organ för bedömning av överensstämmelse gör en överensstämmelsebedömning av de kvalificerade tillhandahållarna av betrodda tjänster på dessa tillhandahållare av betrodda tjänsters egen bekostnad för att bekräfta att dessa och de kvalificerade betrodda tjänster som de tillhandahåller uppfyller kraven i denna förordning. Vid misstänkta överträdelse av reglerna om skydd av personuppgifter ska tillsynsorganet utan onödigt dröjsmål informera de behöriga tillsynsmyndigheterna som inrättats enligt artikel 51 i förordning (EU) 2016/679.

3. Om den kvalificerade tillhandahållaren av betrodda tjänster underlåter att uppfylla kraven i denna förordning ska tillsynsorganet ålägga denna tillhandahållare att åtgärda bristerna inom en fastställd tidsfrist, om tillämpligt.

Om tillhandahållaren inte åtgärdar bristerna, i tillämpliga fall inom den tidsfrist som fastställs av tillsynsorganet, ska tillsynsorganet, i synnerhet när det är motiverat av underlåtenhetens omfattning, varaktighet och följder, återkalla den tillhandahållarens eller den berörda tillhandahållna tjänstens status som kvalificerad.

3a. Om de behöriga myndigheter som utsetts eller inrättats enligt artikel 8.1 i direktiv (EU) 2022/2555 informerar tillsynsorganet om att den kvalificerade tillhandahållaren av betrodda tjänster underlåter att uppfylla kraven i artikel 21 i det direktivet ska tillsynsorganet, i synnerhet när det är motiverat av underlåtenhetens omfattning, varaktighet och följder, återkalla status som kvalificerad för den tillhandahållaren eller den berörda tillhandahållna tjänst som denne tillhandahåller.

3b. Om tillsynsmyndigheterna som inrättats enligt artikel 51 i förordning (EU) 2016/679 informerar tillsynsorganet om att den kvalificerade tillhandahållaren av betrodda tjänster underlåter att uppfylla kraven i den förordningen ska tillsynsorganet, i synnerhet när det är motiverat av underlåtenhetens omfattning, varaktighet och följder, återkalla den tillhandahållarens eller den berörda tillhandahållna tjänstens status som kvalificerad.

3c. Tillsynsorganet ska informera den kvalificerade tillhandahållaren av betrodda tjänster om återkallandet av dess eller den berörda tjänstens status som kvalificerad. Tillsynsorganet ska informera det organ som anmälts i enlighet med artikel 22.3 i denna förordning i syfte att uppdatera de förteckningar över betrodda tjänsteleverantörer som avses i punkt 1 i den artikeln och den behöriga myndighet som utsetts eller inrättats i enlighet med artikel 8.1 i direktiv (EU) 2022/2555.

4. Senast den 21 maj 2025 ska kommissionen, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för följande:

- a) Ackreditering av organ för bedömning av överensstämmelse och för den rapport om bedömning av överensstämmelse som avses i punkt 1.
- b) Granskningskrav för hur organ för bedömning av överensstämmelse ska göra sin bedömning av överensstämmelse, inbegripet sammansatt bedömning, vad gäller kvalificerade tillhandahållare av betrodda tjänster som avses i punkt 1.
- c) De system för bedömning av överensstämmelse som gäller för den bedömning av överensstämmelsen för kvalificerade tillhandahållare av betrodda tjänster som utförs av organ för bedömning av överensstämmelse och för tillhandahållandet av den rapport som avses i punkt 1.

Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.”

20. Artikel 21 ska ändras på följande sätt:

a) Punkterna 1 och 2 ska ersättas med följande:

”1. När tillhandahållare av betrodda tjänster har för avsikt att börja tillhandahålla en kvalificerad betrodd tjänst, ska de anmäla sin avsikt till tillsynsorganet och samtidigt lämna in en rapport om bedömning av överensstämmelse som utfärdats av ett organ för bedömning av överensstämmelse och som bekräftar att kraven i denna förordning och i artikel 21 i direktiv (EU) 2022/2555 är uppfyllda.

2. Tillsynsorganet ska kontrollera huruvida tillhandahållaren av betrodda tjänster och de betrodda tjänster som denne tillhandahåller uppfyller kraven i denna förordning, och i synnerhet kraven för kvalificerade tillhandahållare av betrodda tjänster och för de kvalificerade betrodda tjänster som de tillhandahåller.

För att kontrollera att tillhandahållaren av betrodda tjänster uppfyller de krav som fastställs i artikel 21 i direktiv (EU) 2022/2555 ska tillsynsorganet begära att de behöriga myndigheter som utsetts eller inrättats enligt artikel 8.1 i det direktivet utför tillsynsverksamhet i det avseendet och tillhandahåller information om resultatet utan onödigt dröjsmål och under alla omständigheter inom två månader efter det att denna begäran har mottagits. Om kontrollen inte har slutförts inom två månader från anmälan, ska dessa behöriga myndigheter informera tillsynsorganet om detta och ange orsakerna till förseningen samt när kontrollen beräknas vara slutförd.

Om tillsynsorganet kommer fram till att tillhandahållaren av betrodda tjänster, och de betrodda tjänster som denne tillhandahåller, uppfyller de krav som fastställs i denna förordning, ska tillsynsorganet bevilja tillhandahållaren av betrodda tjänster, och de betrodda tjänster som denne tillhandahåller, status som kvalificerad, samt informera det organ som avses i artikel 22.3 så att de förteckningar över betrodda tjänsteleverantörer som avses i artikel 22.1 kan uppdateras, senast tre månader efter anmälan i enlighet med punkt 1 i denna artikel.

Om kontrollen inte har slutförts inom tre månader från anmälan, ska tillsynsorganet informera tillhandahållaren av betrodda tjänster om detta och ange orsakerna till förseningen samt när kontrollen beräknas vara slutförd."

b) Punkt 4 ska ersättas med följande:

"4. Senast den 21 maj 2025 ska kommissionen genom genomförandeakter fastställa formaten och förfarandena för anmälan och kontroll enligt punkterna 1 och 2 i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2."

21. Artikel 24 ska ändras på följande sätt:

a) Punkt 1 ska ersättas med följande:

"1. En kvalificerad tillhandahållare av betrodda tjänster ska, när den utfärdar ett kvalificerat certifikat eller ett kvalificerat elektroniskt attributsintyg, kontrollera identiteten och, i förekommande fall, eventuella särskilda attribut för den fysiska eller juridiska person till vilken det kvalificerade certifikatet eller det kvalificerade elektroniska attributsintyget ska utfärdas.

1a. Den kontroll av identiteten som avses i punkt 1 ska utföras på lämpligt sätt av den kvalificerade tillhandahållaren av betrodda tjänster, antingen direkt eller med hjälp av en tredje part, på grundval av en av följande metoder eller vid behov en kombination av dessa, i enlighet med de genomförandeakter som avses i punkt 1c:

- a) Genom den europeiska digitala identitetsplånboken eller ett anmält medel för elektronisk identifiering som uppfyller kraven i artikel 8 vad gäller tillitsnivå hög.
- b) Genom ett certifikat för en kvalificerad elektronisk underskrift eller en kvalificerad elektronisk stämpel som utfärdats i enlighet med led a, c eller d.
- c) Genom användning av andra identifieringsmetoder som säkerställer identifiering av personen med en hög tillförlitlighetsnivå, vars överensstämmelse ska ha bekräftats av ett organ för bedömning av överensstämmelse.
- d) Genom fysisk närvaro av den fysiska personen eller av en behörig företrädare för den juridiska personen, med hjälp av lämpliga bevis och förfaranden och i enlighet med nationell rätt.

1b. Den kontroll av attribut som avses i punkt 1 ska utföras på lämpligt sätt av den kvalificerade tillhandahållaren av betrodda tjänster, antingen direkt eller med hjälp av en tredje part, på grundval av en av följande metoder eller vid behov en kombination av dessa, i enlighet med de genomförandeakter som avses i punkt 1c:

- a) Genom den europeiska digitala identitetsplånboken eller ett anmält medel för elektronisk identifiering som uppfyller kraven i artikel 8 vad gäller tillitsnivå hög.

- b) Genom ett certifikat för en kvalificerad elektronisk underskrift eller en kvalificerad elektronisk stämpel som utfärdats i enlighet med punkt 1 a, c eller d.
- c) Genom ett kvalificerat elektroniskt attributsintyg.
- d) Genom användning av andra metoder som säkerställer kontroll av attributen med en hög tillförlitlighetsnivå, vars överensstämmelse ska ha bekräftats av ett organ för bedömning av överensstämmelse.
- e) Genom fysisk närvaro av den fysiska personen eller av en behörig företrädare för den juridiska personen, med hjälp av lämpliga bevis, förfaranden och i enlighet med nationell rätt."

"1c. Senast den 21 maj 2025 ska kommissionen, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för kontrollen av identitet och attribut i enlighet med punkterna 1, 1 a och 1 b i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2."

- b) Punkt 2 ska ändras på följande sätt:

- i) Led a ska ersättas med följande:

"a) informera tillsynsorganet minst en månad innan någon ändring av tillhandahållandet av dess kvalificerade betrodda tjänster genomförs, eller minst tre månader om det finns en avsikt att upphöra med denna verksamhet,".

- ii) Leden d och e ska ersättas med följande:

"d) innan den ingår ett avtalsförhållande, på ett tydligt, uttömmande och lättillgängligt sätt, på en allmänt tillgänglig plats och individuellt, informera de personer som vill använda en kvalificerad betrodd tjänst om de exakta villkor som gäller för användning av den tjänsten, inbegripet om eventuella begränsningar av användningen,

e) använda tillförlitliga system och produkter som är skyddade mot ändringar och säkerställa den tekniska säkerheten och tillförlitligheten hos de processer som stöds av dessa, och även använda lämpliga krypteringstekniker,".

- iii) Följande led ska läggas till:

"fa) trots artikel 21 i direktiv (EU) 2022/2555, ha lämpliga policyer och vidta motsvarande åtgärder för att hantera rättsliga, affärsmässiga, operativa och andra direkta eller indirekta risker för tillhandahållandet av kvalificerade betrodda tjänster, inbegripet åtminstone åtgärder avseende följande:

- i) registrerings- och anslutningsförfaranden för en tjänst,

- ii) förfarandemässiga eller administrativa kontroller,

- iii) förvaltning och genomförande av tjänster,

fb) anmäla till tillsynsorganet, de identifierbara berörda personerna, andra relevanta behöriga organ om tillämpligt och, på begäran av tillsynsorganet, allmänheten om det är av allmänt intresse, alla säkerhetsincidenter eller störningar vid tillhandahållandet av tjänsten eller genomförandet av de åtgärder som avses i led fa i, ii eller iii och som har en betydande inverkan på den tillhandahållna betrodda tjänsten eller de personuppgifter som lagras däri, utan onödigt dröjsmål och under alla omständigheter inom 24 timmar från händelsen,".

- iv) Leden g, h och i ska ersättas med följande:

"g) vidta lämpliga åtgärder mot förfalskning, stöld eller felaktigt förvärv av data eller mot radering, ändring eller otillgängliggörande av data om rättighet till detta saknas,

h) under en så lång tid som är nödvändig efter det att den kvalificerade tillhandahållaren av betrodda tjänster har upphört med sin verksamhet, registrera och tillgängliggöra all relevant information om uppgifter som den kvalificerade tillhandahållaren av betrodda tjänster har utfärdat och tagit emot, för att kunna lägga fram bevis vid rättsliga förfaranden och för att säkerställa tjänstens kontinuitet; registreringen får göras elektroniskt,

i) ha en uppdaterad plan för verksamhetens upphörande i syfte att säkerställa tjänstens kontinuitet i enlighet med bestämmelser som kontrolleras av tillsynsorganet enligt artikel 46b.4 i.”.

v) Led j ska utgå.

vi) Följande stycke ska läggas till:

”Tillsynsorganet får begära information utöver den information som anmälts i enlighet med första stycket a eller resultatet av en bedömning av överensstämmelse och får villkora beviljandet av tillståndet att genomföra de avsedda ändringarna av de kvalificerade betrodda tjänsterna. Om kontrollen inte har slutförts inom tre månader från anmälan, ska tillsynsorganet informera tillhandahållaren av betrodda tjänster om detta och ange orsakerna till förseningen samt när kontrollen beräknas vara slutförd.”.

c) Punkt 5 ska ersättas med följande:

”4a. Punkterna 3 och 4 ska i enlighet med detta tillämpas vid återkallelse av kvalificerade elektroniska attributsintyg.

4b. Kommissionen ska ges befogenhet att anta delegerade akter i enlighet med artikel 47, för fastställande av ytterligare åtgärder som avses i punkt 2 fa i den här artikeln.

5. Senast den 21 maj 2025 ska kommissionen, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för de krav som avses i punkt 2 i denna artikel. Överensstämmelse med kraven i denna punkt i denna artikel ska förutsättas när dessa standarder, specifikationer och förfaranden uppfylls. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.”

22. Följande artikel ska införas i kapitel III, avsnitt 3:

”Artikel 24a

Erkännande av kvalificerade betrodda tjänster

1. Kvalificerade elektroniska underskrifter baserade på ett kvalificerat certifikat som utfärdats i en medlemsstat, och kvalificerade elektroniska stämplar baserade på ett kvalificerat certifikat som utfärdats i en medlemsstat, ska erkännas som kvalificerade elektroniska underskrifter respektive kvalificerade elektroniska stämplar i alla andra medlemsstater.

2. Kvalificerade anordningar för skapande av elektroniska underskrifter och kvalificerade anordningar för skapande av elektroniska stämplor som certifierats i en medlemsstat ska erkännas som kvalificerade anordningar för skapande av elektroniska underskrifter respektive kvalificerade anordningar för skapande av elektroniska stämplor i alla andra medlemsstater.

3. Ett kvalificerat certifikat för elektroniska underskrifter, ett kvalificerat certifikat för elektroniska stämplor, en kvalificerad betrodd tjänst för förvaltning av en kvalificerad anordning för skapande av elektroniska underskrifter på distans och en kvalificerad betrodd tjänst för förvaltning av kvalificerade anordningar för skapande av elektroniska stämplor på distans, tillhandahållna i en medlemsstat, ska erkännas som ett kvalificerat certifikat för elektroniska underskrifter, ett kvalificerat certifikat för elektroniska stämplor, en kvalificerad betrodd tjänst för förvaltning av kvalificerade anordningar för skapande av elektroniska underskrifter på distans och en kvalificerad betrodd tjänst för förvaltning av kvalificerade anordningar för skapande av elektroniska stämplor på distans i alla andra medlemsstater.

4. En kvalificerad valideringstjänst för kvalificerade elektroniska underskrifter och en kvalificerad valideringstjänst för kvalificerade elektroniska stämplor, tillhandahållna i en medlemsstat, ska erkännas som en kvalificerad valideringstjänst för kvalificerade elektroniska underskrifter respektive en kvalificerad valideringstjänst för kvalificerade elektroniska stämplor i alla andra medlemsstater.

5. En kvalificerad tjänst för bevarande av kvalificerade elektroniska underskrifter och en kvalificerad tjänst för bevarande av kvalificerade elektroniska stämplor, tillhandahållna i en medlemsstat, ska erkännas som en kvalificerad tjänst för bevarande av kvalificerade elektroniska underskrifter respektive en kvalificerad tjänst för bevarande av kvalificerade elektroniska stämplor i alla andra medlemsstater.

6. En kvalificerad elektronisk tidsstämpling, tillhandahållen i en medlemsstat, ska erkännas som en kvalificerad elektronisk tidsstämpling i alla andra medlemsstater.

7. Ett kvalificerat certifikat för autentisering av webbplatser, utfärdat i en medlemsstat, ska erkännas som ett kvalificerat certifikat för autentisering av webbplatser i alla andra medlemsstater.
8. En kvalificerad elektronisk tjänst för rekommenderade leveranser, tillhandahållen i en medlemsstat, ska erkännas som en kvalificerad elektronisk tjänst för rekommenderade leveranser i alla andra medlemsstater.
9. Ett kvalificerat elektroniskt attributsintyg, utfärdat i en medlemsstat, ska erkännas som ett kvalificerat elektroniskt attributsintyg i alla andra medlemsstater.
10. En kvalificerad elektronisk arkiveringstjänst, tillhandahållen i en medlemsstat, ska erkännas som en kvalificerad elektronisk arkiveringstjänst i alla andra medlemsstater.
11. En kvalificerad elektronisk liggare, tillhandahållen i en medlemsstat, ska erkännas som en kvalificerad elektronisk liggare i alla andra medlemsstater."
23. Artikel 25.3 ska utgå.
24. Artikel 26 ska ändras på följande sätt:
- a) Det enda stycket ska benämnas punkt 1.
- b) Följande punkt ska läggas till:
- "2. Senast den 21 maj 2026 ska kommissionen bedöma huruvida det är nödvändigt att anta genomförandeakter för att upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för avancerade elektroniska underskrifter. På grundval av resultatet av den bedömningen får kommissionen anta sådana genomförandeakter. Överensstämmelse med kraven för avancerade elektroniska underskrifter ska presumeras om en avancerad elektronisk underskrift överensstämmer med dessa standarder, specifikationer och förfaranden. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2."
25. Artikel 27.4 ska utgå.
26. Artikel 28.6 ska ersättas med följande:
- "6. Senast den 21 maj 2025 ska kommissionen, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för kvalificerade certifikat för elektroniska underskrifter. Överensstämmelse med kraven i bilaga I ska presumeras om ett kvalificerat certifikat för elektroniska underskrifter uppfyller kraven i dessa standarder, specifikationer och förfaranden. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2."
27. I artikel 29 ska följande punkt införas:
- "1a. Generering eller hantering av uppgifter för skapande av elektroniska underskrifter eller kopiering av sådana uppgifter för skapande av underskrifter för framställning av säkerhetskopior får utföras endast för undertecknarens räkning, på undertecknarens begäran, av en kvalificerad tillhandahållare av betrodda tjänster som tillhandahåller en kvalificerad betrodd tjänst för förvaltningen av en kvalificerad anordning för skapande av elektroniska underskrifter på distans."
28. Följande artikel ska införas:
- "Artikel 29a
- Krav för kvalificerade tjänster för förvaltning av kvalificerade anordningar för skapande av elektroniska underskrifter på distans**
1. Förvaltning av kvalificerade anordningar för skapande av elektroniska underskrifter på distans som en kvalificerad tjänst får utföras endast av en kvalificerad tillhandahållare av betrodda tjänster som
- a) genererar eller hanterar uppgifter för skapande av elektroniska underskrifter för undertecknarens räkning,
- b) trots punkt 1 d i bilaga II, kopierar uppgifterna för skapande av elektroniska underskrifter endast för framställning av säkerhetskopior, förutsatt att följande krav uppfylls:
- i) Säkerheten för de kopierade datauppsättningarna måste vara på samma nivå som för de ursprungliga datauppsättningarna.
- ii) Antalet kopierade datauppsättningar får inte överskrida det minsta antal som krävs för att säkerställa tjänstens kontinuitet.

SV

EUT L, 30.4.2024

- c) uppfyller alla krav som anges i certifieringsrapporten för den specifika kvalificerade anordning för skapande av elektroniska underskrifter på distans som utfärdats i enlighet med artikel 30.
2. Senast den 21 maj 2025 ska kommissionen, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, specifikationer och förfaranden för tillämpningen av punkt 1 i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2."
29. I artikel 30 ska följande punkt införas:
- "3a. Giltigheten för den certifiering som avses i punkt 1 får inte överstiga fem år, förutsatt att sårbarhetsbedömningar genomförs vartannat år. Om sårbarheter identifieras och inte åtgärdas ska certifieringen upphöra att gälla."
30. Artikel 31.3 ska ersättas med följande:
- "3. Senast den 21 maj 2025 ska kommissionen genom genomförandeakter fastställa format och förfaranden som ska vara tillämpliga för de ändamål som avses i punkt 1 i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2."
31. Artikel 32 ska ändras på följande sätt:
- a) I punkt 1 ska följande stycke läggas till:
- "Överensstämmelse med kraven i första stycket i denna artikel ska presumeras om valideringen av kvalificerade elektroniska underskrifter följer de standarder, specifikationer och förfaranden som avses i punkt 3."
- b) Punkt 3 ska ersättas med följande:
- "3. Senast den 21 maj 2025 ska kommissionen, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för validering av kvalificerade elektroniska underskrifter. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2."
32. Följande artikel ska införas:
- "Artikel 32a
- Krav för validering av avancerade elektroniska underskrifter baserade på kvalificerade certifikat**
1. Genom valideringsförfarandet för en avancerad elektronisk underskrift baserad på ett kvalificerat certifikat ska giltigheten för en avancerad elektronisk underskrift baserad på ett kvalificerat certifikat bekräftas under förutsättning att
- a) det certifikat som stöder underskriften vid tidpunkten för undertecknandet var ett kvalificerat certifikat för elektroniska underskrifter som överensstämmer med bilaga I,
- b) det kvalificerade certifikatet har utfärdats av en kvalificerad tillhandahållare av betrodda tjänster och var giltigt vid tidpunkten för undertecknandet,
- c) valideringsuppgifterna för underskriften överensstämmer med de uppgifter som lämnats till den förlitande parten,
- d) certifikatets unika uppsättning uppgifter som avser undertecknaren har tillhandahållits den förlitande parten på rätt sätt,
- e) användningen av en eventuell pseudonym tydligt har angetts för den förlitande parten om en pseudonym användes vid tidpunkten för undertecknandet,
- f) integriteten hos de undertecknade uppgifterna inte har äventyrats,
- g) kraven i artikel 26 var uppfyllda vid tidpunkten för undertecknandet.

2. Det system som används för att validera den avancerade elektroniska underskriften baserad på kvalificerade certifikat ska ge den förlitande parten det korrekta resultatet av valideringsförfarandet och ska göra det möjligt för den förlitande parten att upptäcka eventuella problem som är relevanta för säkerheten.

3. Senast den 21 maj 2025 ska kommissionen, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för validering av avancerade elektroniska underskrifter baserade på kvalificerade certifikat. Överensstämmelse med kraven i punkt 1 i denna artikel ska presumeras om valideringen av avancerade elektroniska underskrifter baserade på kvalificerade certifikat uppfyller kraven i dessa standarder, specifikationer och förfaranden. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2."

33. Artikel 33.2 ska ersättas med följande text:

"2. Senast den 21 maj 2025 ska kommissionen, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för den kvalificerade valideringstjänst som avses i punkt 1 i denna artikel. Överensstämmelse med kraven i punkt 1 i denna artikel ska presumeras om den kvalificerade valideringstjänsten för kvalificerade elektroniska underskrifter uppfyller kraven i dessa standarder, specifikationer och förfaranden. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2."

34. Artikel 34 ska ändras på följande sätt:

a) Följande punkt ska införas:

"1a. Överensstämmelse med kraven i punkt 1 ska presumeras om arrangemangen för de kvalificerade tjänsterna för bevarande av kvalificerade elektroniska underskrifter uppfyller kraven i de standarder, specifikationer och förfaranden som avses i punkt 2."

b) Punkt 2 ska ersättas med följande:

"2. Senast den 21 maj 2025 ska kommissionen, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för de kvalificerade tjänsterna för bevarande av kvalificerade elektroniska underskrifter. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2."

35. Artikel 35.3 ska utgå.

36. Artikel 36 ska ändras på följande sätt:

a) Det enda stycket ska benämnas punkt 1.

b) Följande punkt ska läggas till:

"2. Senast den 21 maj 2026 ska kommissionen bedöma huruvida det är nödvändigt att anta genomförandeakter i syfte att upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för avancerade elektroniska stämplat. På grundval av resultatet av den bedömningen får kommissionen anta sådana genomförandeakter. Överensstämmelse med kraven för avancerade elektroniska stämplat ska presumeras om en avancerad elektronisk stämpel uppfyller kraven i dessa standarder, specifikationer och förfaranden. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2."

37. Artikel 37.4 ska utgå.

38. Artikel 38.6 ska ersättas med följande:

"6. Senast den 21 maj 2025 ska kommissionen, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för kvalificerade certifikat för elektroniska stämplat. Överensstämmelse med kraven i bilaga III ska presumeras om ett kvalificerat certifikat för elektroniska stämplat uppfyller kraven i dessa standarder, specifikationer och förfaranden. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2."

39. Följande artikel ska införas:

"Artikel 39a

Krav för kvalificerade tjänster för förvaltning av kvalificerade anordningar för skapande av elektroniska stämplarna på distans

Artikel 29a ska i tillämpliga delar gälla för kvalificerade tjänster för förvaltning av kvalificerade anordningar för skapande av elektroniska stämplarna på distans."

40. Följande artikel ska införas i kapitel III avsnitt 5:

"Artikel 40a

Krav för validering av avancerade elektroniska stämplarna baserade på kvalificerade certifikat

Artikel 32a ska i tillämpliga delar gälla för validering av avancerade elektroniska stämplarna baserade på kvalificerade certifikat."

41. Artikel 41.3 ska utgå.

42. Artikel 42 ska ändras på följande sätt:

a) Följande punkt ska införas:

"1a. Överensstämmelse med kraven i punkt 1 ska presumeras om bindningen av datum och tidpunkt till uppgifter och korrektheten för tidskällan uppfyller kraven i de standarder, specifikationer och förfaranden som avses i punkt 2."

b) Punkt 2 ska ersättas med följande:

"2. Senast den 21 maj 2025 ska kommissionen, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för bindningen av datum och tidpunkt till uppgifter och fastställande av korrektheten för tidskällor. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2."

43. Artikel 44 ska ändras på följande sätt:

a) Följande punkt ska införas:

"1a. Överensstämmelse med kraven i punkt 1 ska presumeras om en process för att sända och ta emot uppgifter uppfyller kraven i de standarder, specifikationer och förfaranden som avses i punkt 2."

b) Punkt 2 ska ersättas med följande:

"2. Senast den 21 maj 2025 ska kommissionen, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för processer för att sända och ta emot uppgifter. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2."

c) Följande punkter ska införas:

"2a. Tillhandahållare av kvalificerade elektroniska tjänster för rekommenderade leveranser får komma överens om interoperabilitet mellan de kvalificerade elektroniska tjänster för rekommenderade leveranser som de tillhandahåller. Ett sådant interoperabilitetsramverk ska uppfylla kraven i punkt 1 och denna uppfyllelse ska bekräftas av ett organ för bedömning av överensstämmelse.

2b. Kommissionen får, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för det interoperabilitetsramverk som avses i punkt 2a i denna artikel. Standarderna ska, vad gäller tekniska specifikationer och innehåll, vara kostnadseffektiva och proportionerliga. Genomförandeakterna ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2."

44. Artikel 45 ska ersättas med följande:

"Artikel 45

Krav på kvalificerade certifikat för autentisering av webbplatser

1. Kvalificerade certifikat för autentisering av webbplatser ska uppfylla de krav som fastställs i bilaga IV. Bedömningen av huruvida dessa krav är uppfyllda ska utföras i enlighet med de standarder, specifikationer och förfaranden som avses i punkt 2 i denna artikel.

1a. Kvalificerade certifikat för autentisering av webbplatser som utfärdats i enlighet med punkt 1 ska erkännas av tillhandahållare av webbläsare. Tillhandahållare av webbläsare ska säkerställa att identitetsuppgifter som intygas i certifikatet och ytterligare intygade attribut visas på ett användarvänligt sätt. Tillhandahållare av webbläsare ska säkerställa stöd och interoperabilitet med kvalificerade certifikat för autentisering av webbplatser enligt punkt 1 i denna artikel, med undantag för mikroföretag eller små företag enligt definitionen i artikel 2 i bilagan till rekommendation 2003/361/EG under de fem första år som de är verksamma som tillhandahållare av webbläsartjänster.

1b. Kvalificerade certifikat för autentisering av webbplatser ska inte omfattas av några obligatoriska krav utöver de krav som fastställs i punkt 1.

2. Senast den 21 maj 2025 ska kommissionen, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för de kvalificerade certifikat för autentisering av webbplatser som avses i punkt 1 i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2."

45. Följande artikel ska införas:

"Artikel 45a

Säkerhetsåtgärder för cybersäkerhet

1. Tillhandahållare av webbläsare ska inte vidta några åtgärder som strider mot deras skyldigheter enligt artikel 45, särskilt kraven på att erkänna kvalificerade certifikat för autentisering av webbplatser och att visa de identitetsuppgifter som tillhandahålls på ett användarvänligt sätt.

2. Genom undantag från punkt 1 och endast vid väl underbyggda farhågor om säkerhetsincidenter eller integritetsförlust hos ett identifierat certifikat eller en identifierad uppsättning certifikat får tillhandahållare av webbläsare vidta säkerhetsåtgärder med avseende på det certifikatet eller den uppsättningen av certifikat.

3. Om en tillhandahållare av en webbläsare vidtar säkerhetsåtgärder enligt punkt 2 ska tillhandahållaren av webbläsaren utan onödigt dröjsmål skriftligen meddela sina farhågor, tillsammans med en beskrivning av de åtgärder som vidtagits för att hantera dessa farhågor, till kommissionen, det behöriga tillsynsorganet, den enhet till vilken certifikatet utfärdades och den kvalificerade tillhandahållare av betrodda tjänster som utfärdade certifikatet eller uppsättningen av certifikat. Vid mottagandet av ett sådant meddelande ska det behöriga tillsynsorganet utfärda ett mottagningsbevis till tillhandahållaren av webbläsaren i fråga.

4. Det behöriga tillsynsorganet ska undersöka de frågor som tas upp i meddelandet i enlighet med artikel 46b.4 k. Om resultatet av utredningen inte leder till att certifikatets status som kvalificerat återkallas ska tillsynsorganet informera tillhandahållaren av webbläsaren om detta och begära att den tillhandahållaren avbryter de säkerhetsåtgärder som avses i punkt 2 i den här artikeln."

46. Följande avsnitt ska läggas till i kapitel III:

"AVSNITT 9

ELEKTRONISKA ATTRIBUTSINTYG

*Artikel 45b***Rättslig verkan av elektroniska attributsintyg**

1. Ett elektroniskt attributsintyg får inte förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att det har elektronisk form eller inte uppfyller kraven för kvalificerade elektroniska attributsintyg.
2. Ett kvalificerat elektroniskt attributsintyg och attributsintyg utfärdade av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa ska ha samma rättsliga verkan som lagligt utfärdade intyg i pappersformat.
3. Ett attributsintyg utfärdat av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa i en medlemsstat ska erkännas som ett attributsintyg utfärdat av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa i alla medlemsstater.

*Artikel 45c***Elektroniska attributsintyg i offentliga tjänster**

I de fall då det enligt nationell rätt krävs elektronisk identifiering med användning av ett medel för elektronisk identifiering och autentisering för åtkomst till en nättjänst som tillhandahålls av ett offentligt organ, ska inte uppgifterna för personidentifiering i det elektroniska attributsintyget ersätta den elektroniska identifieringen med användning av medel för elektronisk identifiering och autentisering om inte detta specifikt tillåts av medlemsstaten. I sådana fall ska kvalificerade elektroniska attributsintyg från andra medlemsstater också godtas.

*Artikel 45d***Krav på kvalificerade elektroniska attributsintyg**

1. Kvalificerade elektroniska attributsintyg ska uppfylla de krav som fastställs i bilaga V.
2. Bedömningen av huruvida kraven i bilaga V är uppfyllda ska utföras i enlighet med de standarder, specifikationer och förfaranden som avses i punkt 5 i denna artikel.
3. Kvalificerade elektroniska attributsintyg ska inte omfattas av några obligatoriska krav utöver de krav som fastställs i bilaga V.
4. Om ett kvalificerat elektroniskt attributsintyg har återkallats efter det ursprungliga utfärdandet, ska det förlora sin giltighet från och med tidpunkten för återkallandet och dess status som giltigt ska inte under några omständigheter återställas.
5. Senast den 21 november 2024 ska kommissionen, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för kvalificerade elektroniska attributsintyg. Dessa genomförandeakter ska vara förenliga med de genomförandeakter som avses i artikel 5a.23 om genomförandet av den europeiska digitala identitetsplanboken. De ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

*Artikel 45e***Kontroll av attribut mot autentiska källor**

1. Medlemsstaterna ska inom 24 månader från dagen för ikraftträdandet av de genomförandeakter som avses i artiklarna 5a.23 och 5c.6, åtminstone för de attribut som förtecknas i bilaga VI när dessa attribut baseras på autentiska källor inom offentliga sektorn, säkerställa att åtgärder vidtas som gör det möjligt för kvalificerade tillhandahållare av betrodda tjänster för elektroniska attributsintyg att på användarens begäran, i enlighet med unionsrätten eller nationell rätt på elektronisk väg kontrollera dessa attribut.
2. Senast den 21 november 2024 ska kommissionen, med beaktande av relevanta internationella standarder, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för katalogen med attribut, liksom system för attributsintyg och kontrollförfaranden för kvalificerade elektroniska attributsintyg för tillämpningen av punkt 1 i denna artikel. Dessa genomförandeakter ska vara förenliga med de genomförandeakter som avses i artikel 5a.23 om genomförandet av den europeiska digitala identitetsplanboken. De ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

*Artikel 45f***Krav på elektroniska attributsintyg utfärdade av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa**

1. Ett elektroniskt attributsintyg utfärdat av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa ska uppfylla följande krav:

a) De som anges i bilaga VII.

b) Det kvalificerade certifikat som stöder den kvalificerade elektroniska underskriften eller den kvalificerade elektroniska stämpeln från det offentliga organ som avses i artikel 3.46 och som identifierats som den utfärdare som avses i led b i bilaga VII, som innehåller en särskild uppsättning certifierade attribut i en form som lämpar sig för automatiserad behandling och

i) som anger att det utfärdande organet är inrättat i enlighet med unionsrätten eller nationell rätt som ansvarigt för den autentiska källa på grundval av vilken det elektroniska attributsintyget utfärdas eller som det organ som utsetts att agera på dess vägnar,

ii) som tillhandahåller en uppsättning uppgifter som otvetydigt avser den autentiska källa som avses i led i, och

iii) som identifierar den unionsrätt eller nationella rätt som avses i led i.

2. Den medlemsstat där de offentliga organ som avses i artikel 3.46 är etablerade ska säkerställa att de offentliga organ som utfärdar elektroniska attributsintyg har en tillförlitlighetsnivå som är likvärdig med den hos kvalificerade tillhandahållare av betrodda tjänster i enlighet med artikel 24.

3. Medlemsstaterna ska underrätta kommissionen om de offentliga organ som avses i artikel 3.46. Denna anmälan ska innehålla en rapport om bedömning av överensstämmelse som utfärdats av ett organ för bedömning av överensstämmelse och som bekräftar att kraven i punkterna 1, 2 och 6 i denna artikel är uppfyllda. Kommissionen ska säkerställa att en förteckning över de offentliga organ som avses i avses i artikel 3.46 genom en säker kanal görs tillgänglig för allmänheten i elektroniskt undertecknad eller stämplad form som lämpar sig för automatiserad behandling.

4. Om ett elektroniskt attributsintyg utfärdat av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa har återkallats efter det ursprungliga utfärdandet ska det förlora sin giltighet från och med tidpunkten för återkallandet, och dess status ska inte återställas.

5. Ett elektroniskt attributsintyg utfärdat av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa ska anses uppfylla kraven i punkt 1 om det uppfyller kraven i de standarder, specifikationer och förfaranden som avses i punkt 6.

6. Senast den 21 november 2024 ska kommissionen, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för ett elektroniskt attributsintyg utfärdat av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa. Dessa genomförandeakter ska vara förenliga med de genomförandeakter som avses i artikel 5a.23 om genomförandet av den europeiska digitala identitetsplånboken. De ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

7. Senast den 21 november 2024 ska kommissionen, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för tillämpningen av punkt 3 i denna artikel. Dessa genomförandeakter ska vara förenliga med de genomförandeakter som avses i artikel 5a.23 om genomförandet av den europeiska digitala identitetsplånboken. De ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

8. Offentliga organ som avses i artikel 3.46 som utfärdar elektroniska attributsintyg ska tillhandahålla ett gränssnitt med de europeiska digitala identitetsplånböcker som utfärdas i enlighet med artikel 5a.

*Artikel 45g***Utfärdande av elektroniska attributsintyg till europeiska digitala identitetsplånböcker**

1. Tillhandahållare av elektroniska attributsintyg ska ge användare av den europeiska digitala identitetsplånböcker möjlighet att begära, erhålla, lagra och hantera det elektroniska attributsintyget, oavsett i vilken medlemsstat den europeiska digitala identitetsplånboken tillhandahålls.

2. Tillhandahållare av kvalificerade elektroniska attributsintyg ska tillhandahålla ett gränssnitt med europeiska digitala identitetsplånböcker som tillhandahålls i enlighet med artikel 5a.

Artikel 45h

Ytterligare regler för tillhandahållande av tjänster för elektroniska attributsintyg

1. Tillhandahållare av kvalificerade och icke-kvalificerade tjänster för elektroniska attributsintyg får inte kombinera personuppgifter som rör tillhandahållandet av dessa tjänster med personuppgifter från några andra tjänster som de eller deras affärspartner erbjuder.

2. Personuppgifter som rör tillhandahållande av tjänster för elektroniska attributsintyg ska hållas logiskt åtskilda från andra data som innehas av tillhandahållaren av elektroniska attributsintyg.

3. Tillhandahållare av tjänster för kvalificerade elektroniska attributsintyg ska genomföra tillhandahållandet av sådana kvalificerade betrodda tjänster på ett sätt som till sin funktion är åtskilt från andra tjänster som de tillhandahåller.

AVSNITT 10

ELEKTRONISKA ARKIVERINGSTJÄNSTER

Artikel 45i

Rättslig verkan av elektroniska arkiveringstjänster

1. Elektroniska uppgifter och elektroniska dokument som bevaras genom en elektronisk arkiveringstjänst får inte förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att de har elektronisk form eller inte är bevarade genom en kvalificerad elektronisk arkiveringstjänst.

2. Elektroniska uppgifter och elektroniska dokument som bevaras genom en kvalificerad elektronisk arkiveringstjänst ska omfattas av en presumtion om deras integritet och ursprung under hela den period som de bevaras av den kvalificerade tillhandahållaren av betrodda tjänster.

Artikel 45j

Krav på kvalificerade elektroniska arkiveringstjänster

1. Kvalificerade elektroniska arkiveringstjänster ska uppfylla följande krav:

- a) De ska tillhandahållas av kvalificerade tillhandahållare av betrodda tjänster.
- b) De ska använda förfaranden och teknik som kan säkerställa att elektroniska uppgifter och elektroniska dokument håller och är läsbara även efter den tekniska giltighetstiden och åtminstone under hela den rättsliga eller avtalsenliga bevarandeperioden, samtidigt som deras integritet och korrekta ursprung bibehålls.
- c) De ska säkerställa att dessa elektroniska uppgifter och elektroniska dokument bevaras på ett sådant sätt att de skyddas mot förlust och ändring, med undantag för ändringar som rör deras medium eller elektroniska format.
- d) De ska göra det möjligt för behöriga förlitande parter att ta emot en rapport på ett automatiserat sätt som bekräftar att elektroniska uppgifter och elektroniska dokument som hämtats från ett kvalificerat elektroniskt arkiv omfattas av presumtionen om uppgifternas integritet från början av bevarandeperioden till tidpunkten för hämtningen.

Den rapport som avses i första stycket led d ska tillhandahållas på ett tillförlitligt och effektivt sätt och ska vara försedd med den kvalificerade elektroniska underskriften eller den kvalificerade elektroniska stämpeln för tillhandahållaren av den kvalificerade elektroniska arkiveringstjänsten.

2. Senast den 21 maj 2025 ska kommissionen, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för kvalificerade elektroniska arkiveringstjänster. Överensstämmelse med kraven på kvalificerade elektroniska arkiveringstjänster ska presumeras om en kvalificerad elektronisk arkiveringstjänst uppfyller kraven i dessa standarder, specifikationer och förfaranden. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2."

AVSNITT 11

ELEKTRONISKA LIGGARE

Artikel 45k

Rättslig verkan av elektroniska liggare

1. En elektronisk liggare får inte förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att den har elektronisk form eller inte uppfyller kraven på kvalificerade elektroniska liggare.
2. Dataloggar i en kvalificerad elektronisk liggare ska omfattas av en presumtion om deras unika och korrekta sekventiella kronologiska ordningsföljd och deras integritet.

Artikel 45l

Krav på kvalificerade elektroniska liggare

1. Kvalificerade elektroniska liggare ska uppfylla följande krav:
 - a) De ska skapas och förvaltas av en eller flera kvalificerade tillhandahållare av betrodda tjänster.
 - b) De ska fastställa ursprunget till dataloggarna i liggaren.
 - c) De ska säkerställa unik sekventiell kronologisk ordning för dataloggarna i liggaren.
 - d) De ska registrera data på ett sådant sätt att alla senare ändringar av uppgifterna omedelbart kan upptäckas, varvid deras integritet säkerställs över tid.
2. Uppfyllelse av kraven i punkt 1 ska presumeras om en elektronisk liggare uppfyller kraven i de standarder, specifikationer och förfaranden som avses i punkt 3.
3. Senast den 21 maj 2025 ska kommissionen, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för de krav som fastställs i punkt 1 i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2."

47. Följande kapitel ska införas:

"KAPITEL IVA

STYRNINGSRAMVERK

Artikel 46a

Tillsyn över ramverket för den europeiska digitala identitetsplånboken

1. Medlemsstaterna ska utse ett eller flera tillsynsorgan som är etablerade på deras territorium.

De tillsynsorgan som utses enligt första stycket ska ges nödvändiga befogenheter och adekvata resurser för att de ska kunna utföra sina uppgifter på ett ändamålsenligt, effektivt och oberoende sätt.
2. Medlemsstaterna ska till kommissionen anmäla namn och adresser för de tillsynsorgan som utsetts enligt punkt 1 och eventuella senare ändringar av dessa. Kommissionen ska offentliggöra en förteckning över de anmälda tillsynsorganen.
3. De tillsynsorgan som utsetts enligt punkt 1 ska ha följande roll:
 - a) Utöva tillsyn över tillhandahållare av europeiska digitala identitetsplånböcker etablerade i den medlemsstat där de har utsetts och, genom tillsynsverksamhet på förhand och i efterhand, säkerställa att dessa tillhandahållare och de europeiska digitala identitetsplånböcker som de tillhandahåller uppfyller kraven i denna förordning.
 - b) Vid behov vidta åtgärder med avseende på tillhandahållare av europeiska digitala identitetsplånböcker etablerade på territoriet för den medlemsstat som utsett den, genom tillsynsverksamhet i efterhand, när de informeras om att tillhandahållarna eller de europeiska digitala identitetsplånböcker som de tillhandahåller inte uppfyller kraven i denna förordning.

4. Uppgifterna för det tillsynsorgan som utsetts enligt punkt 1 ska särskilt inbegripa följande:
- a) Samarbeta med andra tillsynsorgan och bistå dem i enlighet med artiklarna 46c och 46e.
 - b) Begära information som är nödvändig för att övervaka efterlevnaden av denna förordning.
 - c) Informera de relevanta behöriga myndigheter som utsetts eller inrättats enligt artikel 8.1 i direktiv (EU) 2022/2555 i berörda medlemsstater om alla betydande säkerhetsincidenter eller integritetsförluster som de får kännedom om vid utförandet av sina uppgifter och, i händelse av en betydande säkerhetsincident eller integritetsförlust som berör andra medlemsstater, informera den gemensamma kontaktpunkt som utsetts eller inrättats enligt artikel 8.3 i direktiv (EU) 2022/2555 i den berörda medlemsstaten och de gemensamma kontaktpunkter som utsetts i enlighet med artikel 46c.1 i denna förordning i övriga berörda medlemsstater, och informera allmänheten eller kräva att tillhandahållare av europeiska digitala identitetsplånböcker gör detta om tillsynsorganet slår fast att ett avslöjande av säkerhetsincidenten eller integritetsförlusten skulle ligga i allmänhetens intresse.
 - d) Utföra inspektioner på plats och utöva tillsyn på distans.
 - e) Kräva att tillhandahållare av europeiska digitala identitetsplånböcker åtgärdar varje underlåtenhet att uppfylla kraven i denna förordning.
 - f) Tillfälligt eller permanent upphäva registreringen och inkluderingen av förlitande parter i den mekanism som avses i artikel 5b.7 vid olaglig eller bedräglig användning av den europeiska digitala identitetsplånboken.
 - g) Samarbeta med behöriga tillsynsmyndigheter som inrättats enligt artikel 51 i förordning (EU) 2016/679, särskilt genom att utan onödigt dröjsmål informera dem vid misstänkta överträdelse av reglerna om skydd av personuppgifter, och om säkerhetsincidenter som förefaller utgöra personuppgiftsincidenter.
5. Om det tillsynsorgan som utsetts enligt punkt 1 kräver att tillhandahållaren av en europeisk digital identitetsplånbok åtgärdar en underlåtenhet att uppfylla kraven enligt denna förordning i enlighet med punkt 4 e, och tillhandahållaren inte agerar i enlighet med detta och, i tillämpliga fall, inom en tidsfrist som fastställts av det tillsynsorganet, får det tillsynsorgan som utsetts enligt punkt 1, särskilt med beaktande av denna underlåtenhets omfattning, varaktighet och följder, ålägga tillhandahållaren att tillfälligt eller permanent upphöra med tillhandahållandet av den europeiska digitala identitetsplånboken. Tillsynsorganet ska utan onödigt dröjsmål informera tillsynsorganen i övriga medlemsstater, kommissionen, förlitande parter och användare av den europeiska digitala identitetsplånboken om beslutet att kräva att tillhandahållandet av den europeiska digitala identitetsplånboken tillfälligt eller permanent upphör.
6. Senast den 31 mars varje år ska varje tillsynsorgan som utsetts enligt punkt 1 överlämna en rapport om det föregående kalenderårets huvudverksamhet till kommissionen. Kommissionen ska göra de årliga rapporterna tillgängliga för Europaparlamentet och rådet.
7. Senast den 21 maj 2025 ska kommissionen genom genomförandeakter fastställa formaten och förfarandena för den rapport som avses i punkt 6 i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 46b

Tillsyn över betrodda tjänster

1. Medlemsstaterna ska utse ett tillsynsorgan som är etablerat på deras territorium eller utse, efter ömsesidig överenskommelse med en annan medlemsstat, ett tillsynsorgan som är etablerat i den andra medlemsstaten. Det tillsynsorganet ska ansvara för tillsynsuppgifter i den medlemsstat som utsett organet vad gäller betrodda tjänster.

De tillsynsorgan som utses enligt första stycket ska ges nödvändiga befogenheter och adekvata resurser för att de ska kunna utföra sina uppgifter.

2. Medlemsstaterna ska till kommissionen anmäla namn och adresser för de tillsynsorgan som utsetts enligt punkt 1 och eventuella senare ändringar av dessa. Kommissionen ska offentliggöra en förteckning över de anmälda tillsynsorganen.

3. De tillsynsorgan som utses enligt punkt 1 ska ha följande roll:
- Utöva tillsyn över kvalificerade tillhandahållare av betrodda tjänster som är etablerade i den medlemsstat där de har utsetts och, genom tillsynsverksamhet på förhand och i efterhand, säkerställa att de kvalificerade tillhandahållarna av betrodda tjänster och de kvalificerade betrodda tjänster som de tillhandahåller uppfyller kraven i denna förordning.
 - Vid behov vidta åtgärder avseende icke-kvalificerade tillhandahållare av betrodda tjänster som är etablerade i den medlemsstat där de har utsetts genom tillsynsverksamhet i efterhand om de tar del av påståenden att dessa icke-kvalificerade tillhandahållare av betrodda tjänster eller de betrodda tjänster som de tillhandahåller inte uppfyller kraven i denna förordning.
4. Uppgifterna för det tillsynsorgan som utsetts enligt punkt 1 ska särskilt inbegripa följande:
- Informera de relevanta behöriga myndigheter som utsetts eller inrättats enligt artikel 8.1 i direktiv (EU) 2022/2555 i de berörda medlemsstaterna om alla betydande säkerhetsincidenter eller integritetsförluster som de får kännedom om under utförandet av sina uppgifter och, i händelse av en betydande säkerhetsincident eller integritetsförlust som berör andra medlemsstater, informera den gemensamma kontaktpunkt som utsetts eller inrättats enligt artikel 8.3 i direktiv (EU) 2022/2555 i den berörda medlemsstaten och de gemensamma kontaktpunkter som utsetts enligt artikel 46c.1 i denna förordning i övriga berörda medlemsstater, och informera allmänheten eller kräva att tillhandahållaren av betrodda tjänster gör detta om tillsynsorganet slår fast att ett avslöjande av säkerhetsincidenten eller integritetsförlusten skulle ligga i allmänhetens intresse.
 - Samarbeta med andra tillsynsorgan och bistå dem i enlighet med artiklarna 46c och 46e.
 - Analysera de rapporter om bedömning av överensstämmelse som avses i artiklarna 20.1 och 21.1.
 - Rapportera till kommissionen om sin huvudverksamhet i enlighet med punkt 6 i denna artikel.
 - Granska eller begära att ett organ för bedömning av överensstämmelse gör en bedömning av överensstämmelse avseende kvalificerade tillhandahållare av betrodda tjänster i enlighet med artikel 20.2.
 - Samarbeta med behöriga tillsynsmyndigheter som inrättats enligt artikel 51 i förordning (EU) 2016/679, särskilt genom att utan onödigt dröjsmål informera dem vid misstänkta överträdelser av reglerna om skydd av personuppgifter, och om säkerhetsincidenter som förefaller utgöra personuppgiftsincidenter.
 - Bevilja status som kvalificerad tillhandahållare av betrodda tjänster och till de tjänster som de tillhandahåller samt återkalla denna status i enlighet med artiklarna 20 och 21.
 - Informera det organ som är ansvarigt för den nationella förteckning över tillhandahållare av betrodda tjänster som avses i artikel 22.3 om sina beslut om beviljande eller återkallande av status som kvalificerad, såvida inte det organet även är det tillsynsorgan som utsetts enligt punkt 1 i denna artikel.
 - Kontrollera befintlighet och korrekt tillämpning av bestämmelser om planer för verksamhetens upphörande i sådana fall när den kvalificerade tillhandahållaren av betrodda tjänster upphör med sin verksamhet, inbegripet hur information hålls tillgänglig i enlighet med artikel 24.2 h.
 - Kräva att tillhandahållare av betrodda tjänster åtgärdar varje underlåtenhet att uppfylla kraven i denna förordning.
 - Undersöka påståenden från tillhandahållare av webbbläsare enligt artikel 45a och vid behov vidta åtgärder.
5. Medlemsstaterna får kräva att det tillsynsorgan som utsetts enligt punkt 1 inrättar, underhåller och uppdaterar en infrastruktur för betrodda tjänster i enlighet med nationell rätt.
6. Senast den 31 mars varje år ska varje tillsynsorgan som utsetts enligt punkt 1 överlämna en rapport om det föregående kalenderårets huvudverksamhet till kommissionen. Kommissionen ska göra de årliga rapporterna tillgängliga för Europaparlamentet och rådet.

7. Senast den 21 maj 2025 ska kommissionen anta riktlinjer för utövningen, av det tillsynsorgan som utsetts enligt punkt 1 i denna artikel, av de uppgifter som avses i punkt 4 i denna artikel och, genom genomförandeakter, fastställa format och förfaranden för den rapport som avses i punkt 6 i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 46c

Gemensamma kontaktpunkter

1. Varje medlemsstat ska utse en gemensam kontaktpunkt för betrodda tjänster, europeiska digitala identitetsplånböcker och anmälda system för elektronisk identifiering.
2. Varje gemensam kontaktpunkt ska utöva en sambandsfunktion för att underlätta gränsöverskridande samarbete mellan tillsynsorganen för tillhandahållare av betrodda tjänster och mellan tillsynsorganen för tillhandahållare av europeiska digitala identitetsplånböcker och, när så är lämpligt, med kommissionen och Europeiska unionens cybersäkerhetsbyrå (Enisa) och med andra behöriga myndigheter i sin medlemsstat.
3. Varje medlemsstat ska offentliggöra och utan onödigt dröjsmål meddela kommissionen namnen på och adresserna till den gemensamma kontaktpunkt som utsetts enligt punkt 1 och eventuella senare ändringar av denna.
4. Kommissionen ska offentliggöra en förteckning över den gemensamma kontaktpunkt som utsetts enligt punkt 3.

Artikel 46d

Ömsesidigt bistånd

1. För att underlätta tillsynen och efterlevnaden av skyldigheterna enligt denna förordning får de tillsynsorgan som utsetts enligt artikel 46a.1 och 46b.1, bland annat genom den samarbetsgrupp som inrättats enligt artikel 46e.1, söka ömsesidigt bistånd från tillsynsorganen i en annan medlemsstat där tillhandahållaren av den europeiska digitala identitetsplånboken eller tillhandahållaren av betrodda tjänster är etablerad, eller där dennes nätverks- och informationssystem är belägna eller dess tjänster tillhandahålls.
2. Det ömsesidiga biståndet ska åtminstone innebära att
 - a) det tillsynsorgan som tillämpar tillsyns- och verkställighetsåtgärder i en medlemsstat ska informera och samråda med tillsynsorganet i den andra berörda medlemsstaten,
 - b) ett tillsynsorgan får begära att tillsynsorganet i en annan berörd medlemsstat vidtar tillsyns- eller verkställighetsåtgärder, till exempel begäranden om att utföra inspektioner i samband med de rapporter om bedömning av överensstämmelse som avses i artiklarna 20 och 21 avseende tillhandahållandet av betrodda tjänster,
 - c) vid behov får tillsynsorganen genomföra gemensamma utredningar tillsammans med tillsynsmyndigheterna i andra medlemsstater.

De berörda medlemsstaterna ska i enlighet med sin nationella rätt besluta om och inrätta arrangemangen och förfarandena för gemensamma åtgärder enligt första stycket.

3. Ett tillsynsorgan till vilket en begäran om bistånd riktas får vägra att tillmötesgå denna begäran på grundval av något av följande skäl:

- a) Det begärda biståndet står inte i proportion till den tillsynsverksamhet som tillsynsorganet utför i enlighet med artiklarna 46a och 46b.
- b) Tillsynsorganet är inte behörigt att tillhandahålla det begärda biståndet.
- c) Det skulle stå i strid med denna förordning att tillhandahålla det begärda biståndet.

4. Senast den 21 maj 2025 och därefter vartannat år ska den samarbetsgrupp som inrättats enligt artikel 46e.1 utfärda riktlinjer om organisatoriska aspekter och förfaranden för det ömsesidiga bistånd som avses i punkterna 1 och 2 i den här artikeln.

*Artikel 46e***Den europeiska samarbetsgruppen för digital identitet**

1. För att stödja och underlätta medlemsstaternas gränsöverskridande samarbete och informationsutbyte om betrodda tjänster, europeiska digitala identitetsplånböcker och anmälda system för elektronisk identifiering ska kommissionen inrätta en europeisk samarbetsgrupp för digital identitet (*samarbetsgruppen*).
2. Samarbetsgruppen ska bestå av företrädare som utnämns av medlemsstaterna och av kommissionen. Samarbetsgruppen ska ledas av kommissionen. Kommissionen ska tillhandahålla samarbetsgruppens sekretariat.
3. Företrädare för berörda parter får, på ad hoc-basis, inbjudas att närvara vid samarbetsgruppens möten och delta i dess arbete som observatörer.
4. Enisa ska bjudas in att delta som observatör i samarbetsgruppens arbete när den utbyter åsikter, bästa praxis och information om relevanta cybersäkerhetsaspekter såsom anmälan av säkerhetsincidenter, och när användning av cybersäkerhetscertifikat eller cybersäkerhetsstandarder behandlas.
5. Samarbetsgruppen ska ha följande uppgifter:
 - a) Utbyta råd och samarbeta med kommissionen om nya politiska initiativ på området digitala identitetsplånböcker, medel för elektronisk identifiering och betrodda tjänster.
 - b) Vid behov ge kommissionen råd vid utarbetandet av utkast till genomförandeakter och delegerade akter som ska antas enligt denna förordning.
 - c) För att stödja tillsynsorganens genomförande av bestämmelserna i denna förordning:
 - i) Utbyta bästa praxis och information om genomförandet av bestämmelserna i denna förordning.
 - ii) Bedöma den relevanta utvecklingen inom sektorerna för digitala identitetsplånböcker, elektronisk identifiering och betrodda tjänster.
 - iii) Anordna gemensamma möten med relevanta intressenter från hela unionen för att diskutera samarbetsgruppens verksamhet och inhämta synpunkter på framväxande politiska utmaningar.
 - iv) Med stöd av Enisa utbyta åsikter, bästa praxis och information om relevanta cybersäkerhetsaspekter när det gäller europeiska digitala identitetsplånböcker, system för elektronisk identifiering och betrodda tjänster.
 - v) Utbyta bästa praxis om utarbetande och genomförande av strategier för anmälan av säkerhetsincidenter, och gemensamma åtgärder enligt artiklarna 5e och 10.
 - vi) Anordna gemensamma möten med den samarbetsgrupp för nät- och informations säkerhet som inrättats enligt artikel 14.1 i direktiv (EU) 2022/2555 för att utbyta relevant information om betrodda tjänster och elektronisk identifiering som är relaterade till cyberhot, incidenter, sårbarheter, medvetandehöjande initiativ, utbildning, övningar och kompetens, kapacitetssupplyggnad, kapacitet för standarder och tekniska specifikationer samt standarder och tekniska specifikationer.
 - vii) På begäran av ett tillsynsorgan diskutera specifika begäranden om ömsesidigt bistånd enligt artikel 46d.
 - viii) Underlätta informationsutbytet mellan tillsynsorganen genom att ge vägledning om organisatoriska aspekter och förfaranden för det ömsesidiga bistånd som avses i artikel 46d.
 - d) Anordna sakkunnigbedömningar av system för elektronisk identifiering som ska anmälas enligt denna förordning.
6. Medlemsstaterna ska säkerställa att deras utsedda företrädare samarbetar på ett effektivt och ändamålsenligt sätt i samarbetsgruppen.

7. Senast den 21 maj 2025 ska kommissionen genom genomförandeakter införa de nödvändiga förfarandemässiga arrangemangen för att främja samarbete mellan medlemsstaterna enligt punkt 5 d i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2."

48. Artikel 47 ska ändras på följande sätt:

a) Punkterna 2 och 3 ska ersättas med följande:

"2. Den befogenhet att anta delegerade akter som avses i artiklarna 5c.7, 24.4b och 30.4 ska ges till kommissionen tills vidare från och med den 17 september 2014.

3. Den delegering av befogenhet som avses i artiklarna 5c.7, 24.4b och 30.4 får när som helst återkallas av Europaparlamentet eller rådet. Ett beslut om återkallelse innebär att delegeringen av den befogenhet som anges i beslutet upphör att gälla. Beslutet får verkan dagen efter det att det offentliggörs i *Europeiska unionens officiella tidning*, eller vid ett senare i beslutet angivet datum. Det påverkar inte giltigheten av delegerade akter som redan har trätt i kraft."

b) Punkt 5 ska ersättas med följande:

"5. En delegerad akt som antas enligt artikel 5c.7, 24.4b eller 30.4 ska träda i kraft endast om varken Europaparlamentet eller rådet har gjort invändningar mot den delegerade akten inom en period av två månader från den dag då akten delgavs Europaparlamentet och rådet, eller om både Europaparlamentet och rådet, före utgången av den perioden, har underrättat kommissionen om att de inte kommer att invända. Denna period ska förlängas med två månader på Europaparlamentets eller rådets initiativ."

49. Följande artikel ska införas i kapitel VI:

"Artikel 48a

Rapporteringskrav

1. Medlemsstaterna ska säkerställa att det samlas in statistik om hur europeiska digitala identitetsplånböcker och de kvalificerade betrodda tjänster som tillhandahålls på deras territorium används.

2. Den statistik som samlas in i enlighet med punkt 1 ska omfatta följande:

a) Antalet fysiska och juridiska personer som har en giltig europeisk digital identitetsplånbok.

b) Antalet och typen av tjänster som godtar användning av den europeiska digitala identitetsplånboken.

c) Antalet klagomål från användare och konsumentskydds- eller dataskyddsincidenter som rör förlitande parter och kvalificerade betrodda tjänster.

d) En sammanfattande rapport med uppgifter om incidenter som hindrar användningen av den europeiska digitala identitetsplånboken.

e) En sammanfattning av betydande säkerhetsincidenter, dataöverträdelser och berörda användare av europeiska digitala identitetsplånböcker eller kvalificerade betrodda tjänster.

3. Den statistik som avses i punkt 2 ska göras tillgänglig för allmänheten i ett öppet och allmänt använt maskinläsbart format.

4. Senast den 31 mars varje år ska medlemsstaterna lämna en rapport om den statistik som samlats in i enlighet med punkt 2 till kommissionen."

50. Artikel 49 ska ersättas med följande:

"Artikel 49

Översyn

1. Kommissionen ska senast den 21 maj 2026 göra en översyn över denna förordnings tillämpning och rapportera resultaten till Europaparlamentet och rådet. I den rapporten ska kommissionen särskilt utvärdera huruvida det är lämpligt att ändra denna förordnings tillämpningsområde eller dess särskilda bestämmelser, inbegripet särskilt bestämmelserna i artikel 5c.5, med beaktande av den erfarenhet som erhållits vid tillämpningen av denna förordning samt den tekniska och rättsliga utvecklingen och marknadsutvecklingen. Rapporten ska vid behov åtföljas av ett förslag till ändringar av denna förordning.
2. Den rapport som avses i punkt 1 ska innehålla en bedömning av tillgängligheten, säkerheten och användbarheten för de anmälda elektroniska medel för identifiering och de europeiska digitala identitetsplånböcker som omfattas av denna förordning, och bedöma om alla privata tillhandahållare av nättjänster som använder sig av tredje parts tjänster för elektronisk identifiering för användarautentisering ska åläggas att godta användningen av anmälda medel för elektronisk identifiering och den europeiska digitala identitetsplånboken.
3. Senast den 21 maj 2030 och vart fjärde år därefter ska kommissionen lämna den rapport som avses i första stycket till Europaparlamentet och rådet om de framsteg som gjorts i förhållande till denna förordnings mål."

51. Artikel 51 ska ersättas med följande:

"Artikel 51

Övergångsbestämmelser

1. Säkra anordningar för skapande av underskrifter för vilka överensstämmelsen har fastställts i enlighet med artikel 3.4 i direktiv 1999/93/EG ska även fortsättningsvis anses vara kvalificerade anordningar för skapande av elektroniska underskrifter enligt denna förordning fram till och med den 21 maj 2027.
2. Kvalificerade certifikat som utfärdas till fysiska personer enligt direktiv 1999/93/EG ska även fortsättningsvis anses som kvalificerade certifikat för elektroniska underskrifter enligt denna förordning fram till och med den 21 maj 2026.
3. Förvaltning av kvalificerade anordningar för skapande av elektroniska underskrifter och stämplrar på distans som utförs av andra kvalificerade tillhandahållare av betrodda tjänster än sådana kvalificerade tillhandahållare av betrodda tjänster som tillhandahåller kvalificerade betrodda tjänster för förvaltning av kvalificerade anordningar för skapande av elektroniska underskrifter och stämplrar på distans i enlighet med artiklarna 29a och 39a får utföras utan att status som kvalificerad för tillhandahållandet av dessa förvaltningstjänster behöver erhållas förrän den 21 maj 2026.
4. Kvalificerade tillhandahållare av betrodda tjänster som har beviljats status som kvalificerad enligt denna förordning före den 20 maj 2024 ska lämna in en rapport om bedömning av överensstämmelse till tillsynsorganet som styrker överensstämmelse med artikel 24.1, 24.1a och 24.1b så snart som möjligt och i alla händelser senast den 21 maj 2026."

52. Bilagorna I–IV ska ändras i enlighet med bilagorna I–IV till den här förordningen.

53. Nya bilagor V, VI och VII ska läggas till i enlighet med bilagorna V, VI och VII till den här förordningen.

Artikel 2

Ikraftträdande

Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den 11 april 2024.

På Europaparlamentets vägnar

R. METSOLA

Ordförande

På rådets vägnar

H. LAHBIB

Ordförande

SV

EUT L, 30.4.2024

BILAGA I

I bilaga I till förordning (EU) nr 910/2014 ska led i ersättas med följande:

"i) Information om det kvalificerade certifikatets giltighet, eller uppgift om var de tjänster som kan användas för att göra förfrågningar om det kvalificerade certifikatets giltighet är lokaliserade."

BILAGA II

I bilaga II till förordning (EU) nr 910/2014 ska punkterna 3 och 4 utgå.

SV

EUT L, 30.4.2024

BILAGA III

I bilaga III till förordning (EU) nr 910/2014 ska led i ersättas med följande:

"i) Information om det kvalificerade certifikatets giltighet, eller uppgift om var de tjänster som kan användas för att göra förfrågningar om det kvalificerade certifikatets giltighet är lokaliserade."

BILAGA IV

Bilaga IV till förordning (EU) nr 910/2014 ska ändras på följande sätt:

1. Led c ska ersättas med följande:

- "c) För fysiska personer: åtminstone namnet på den person som certifikatet utfärdats till eller en pseudonym; om en pseudonym används ska detta tydligt anges.
- ca) För juridiska personer: en unik uppsättning uppgifter som otvetydigt avser den juridiska person som certifikatet utfärdats till, med åtminstone namnet på den juridiska person som intyget utfärdats till och, i förekommande fall, registreringsnummer i enlighet med vad som uppgetts i de officiella registren."

2. Led j ska ersättas med följande:

- "j) Information om det kvalificerade certifikatets giltighet, eller uppgift om var de tjänster som kan användas för att göra förfrågningar om det kvalificerade certifikatets giltighet är lokaliserade."
-

BILAGA V

"BILAGA V

KRAV PÅ KVALIFICERADE ELEKTRONISKA ATTRIBUTSINTYG

Kvalificerade elektroniska attributsintyg ska innehålla följande:

- a) En uppgift, åtminstone i en form som lämpar sig för automatiserad behandling, om att intyget har utfärdats som ett kvalificerat elektroniskt attributsintyg.
- b) En uppsättning uppgifter som otvetydigt avser den kvalificerade tillhandahållare av betrodda tjänster som utfärdar det kvalificerade elektroniska attributsintyget, inbegripet uppgift om åtminstone vilken medlemsstat tillhandahållaren är etablerad i, samt
 - i) för en juridisk person: namn och, i tillämpliga fall, registreringsnummer i enlighet med vad som uppgetts i de officiella handlingarna,
 - ii) för en fysisk person: personens namn.
- c) En uppsättning uppgifter som otvetydigt avser den enhet som de intygade attributen hänvisar till; om en pseudonym används ska detta anges tydligt.
- d) Det intygade attributet eller de intygade attributen, inbegripet, i tillämpliga fall, de uppgifter som är nödvändiga för att fastställa omfattningen för dessa attribut.
- e) Detaljerade uppgifter om när intyget börjar respektive upphör att gälla.
- f) Intygets identitetskod, vilken måste vara unik för den kvalificerade tillhandahållaren av betrodda tjänster, och, i tillämpliga fall, uppgift om det intygssystem som attributsintyget omfattas av.
- g) Den kvalificerade elektroniska underskriften eller den kvalificerade elektroniska stämpeln för den utfärdande kvalificerade tillhandahållaren av betrodda tjänster.
- h) Uppgift om var det certifikat som stöder den kvalificerade elektroniska underskrift eller den kvalificerade elektroniska stämpel som avses i led g är tillgängligt kostnadsfritt.
- i) Information om det kvalificerade intygets giltighet, eller uppgift om var de tjänster som kan användas för att göra förfrågningar är lokaliserade."

BILAGA VI

"BILAGA VI

MINIMIFÖRTECKNING ÖVER ATTRIBUT

Enligt artikel 45e ska medlemsstaterna säkerställa att åtgärder vidtas för att göra det möjligt för kvalificerade tillhandahållare av betrodda tjänster som tillhandahåller elektroniska attributsintyg att på användarens begäran på elektronisk väg kontrollera äktheten hos följande attribut gentemot den relevanta autentiska källan på nationell nivå eller via särskilt utsedda mellanhänder som är erkända på nationell nivå, i enlighet med unionsrätten eller nationell rätt och i de fall då dessa attribut utgår från autentiska källor inom den offentliga sektorn:

1. Adress.
2. Ålder.
3. Kön.
4. Civilstånd.
5. Familjesammansättning.
6. Nationalitet eller medborgarskap.
7. Utbildningskvalifikationer, titlar och licenser.
8. Yrkeskvalifikationer, titlar och licenser.
9. Befogenheter och uppdrag att företräda fysiska eller juridiska personer
10. Offentliga tillstånd och licenser.
11. För juridiska personer, finansiella uppgifter och företagsuppgifter."

BILAGA VII

"BILAGA VII

KRAV PÅ ELEKTRONISKA INTYG PÅ ATTRIBUT UTFÄRDADE AV ELLER PÅ UPPDRAG AV ETT OFFENTLIGT ORGAN
SOM ANSVARAR FÖR EN AUTENTISK KÄLLA

Ett elektroniskt attributsintyg utfärdat av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa ska innehålla följande:

- a) En uppgift, åtminstone i en form som lämpar sig för automatiserad behandling, om att intyget har utfärdats som ett elektroniskt attributsintyg utfärdat av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa.
- b) En uppsättning uppgifter som otvetydigt avser det offentliga organ som utfärdar det elektroniska attributsintyget, inbegripet åtminstone den medlemsstat där det offentliga organet är etablerat och dess namn och, i tillämpliga fall, dess registreringsnummer i enlighet med vad som anges i de officiella registren.
- c) En uppsättning uppgifter som otvetydigt avser den enhet som de intygade attributen hänvisar till; om en pseudonym används ska detta anges tydligt.
- d) Det intygade attributet eller de intygade attributen, inbegripet, i tillämpliga fall, de uppgifter som är nödvändiga för att fastställa omfattningen för dessa attribut.
- e) Detaljerade uppgifter om när intyget börjar respektive upphör att gälla.
- f) Intygets identitetskod, vilken måste vara unik för det utfärdande offentliga organet, och, i tillämpliga fall, uppgift om det intygssystem som attributsintyget omfattas av.
- g) Det utfärdande organets kvalificerade elektroniska underskrift eller kvalificerade elektroniska stämpel.
- h) Uppgift om var det certifikat som stöder den kvalificerade elektroniska underskrift eller den kvalificerade elektroniska stämpel som avses i led g är tillgängligt kostnadsfritt.
- i) Information om intygets giltighet, eller uppgift om var de tjänster som kan användas för att göra förfrågningar om intygets giltighet är lokaliserade."

Författningar med hänvisning till EU:s förordning om elektronisk identifiering

Statisk hänvisning

- 12 kap. 8 § rättegångsbalken
- 17 kap. 10 § rättegångsbalken
- 30 kap. 8 § rättegångsbalken
- 33 kap. 1 a § rättegångsbalken
- 48 kap. 9 § rättegångsbalken
- 48 kap. 17 § rättegångsbalken
- 111 kap. 5 § socialförsäkringsbalken
- 3 § lagen (1969:12) om internationell vägtransport
- 4 kap. 3 § lagen (1974:371) om rättegången i arbetstvister
- 8 a § lagen (1974:610) om inrikes vägtransport
- 34 § hyresförhandlingslagen (1978:304)
- 11 § lagen (1978:599) om avbetalningsköp mellan näringsidkare m.fl.
- 1 kap. 4 § sparbankslagen (1987:619)
- 19 § lagen (1990:746) om betalningsföreläggande och handräckning
- 1 kap. 9 § stiftelselagen (1994:1220)
- 2 kap. 7 § årsredovisningslagen (1995:1554)
- 2 a § revisionslagen (1999:1079)
- 1 kap. 13 § aktiebolagslagen (2005:551)
- 5 kap. 4 § lagen (2010:921) om mark- och miljödomstolar
- 43 § konsumentkreditlagen (2010:1846)

- 10 kap. 3 § lagen (2011:1029) om upphandling på försvars- och säkerhetsområdet
- 11 § skuldsaneringslagen (2016:675)
- 12 § lagen (2016:676) om skuldsanering för företagare
- 5 kap. 8 § lagen (2016:977) om kollektiv förvaltning av upphovsrätt
- 12 kap. 7 § lagen (2016:1146) om upphandling inom försörjningssektorerna
- 10 kap. 7 § lagen (2016:1147) om upphandling av koncessioner
- 26 § lagen (2018:90) om insyn i finansiering av partier
- 1 kap. 15 § lagen (2018:672) om ekonomiska föreningar
- 2 kap. 5 § lagen (2021:401) om Allmänna arvsfonden
- 3 kap. 5 § fastighetsmäklarlagen (2021:516)
- 2 kap. 3 § lagen (2022:964) om företagsrekonstruktion
- 5 kap. 2 § lagen (2022:1746) med kompletterande bestämmelser till EU:s förordning om en paneuropeisk privat pensionsprodukt (PEPP-produkt)
- 9 a § förordningen (1982:805) om ersättning av allmänna medel till vittnen, m.m.
- 24 § förordningen (1996:271) om mål och ärenden i allmän domstol
- 1 kap. 5 a § förordningen (2004:329) om bank- och finansieringsrörelse
- 4 kap. 2 a § aktiebolagsförordningen (2005:559)
- 13 a § förordningen (2005:1095) om ärenden i arrendenämnd och hyresnämnd
- 12 § förordningen (2013:390) om mål i allmän förvaltningsdomstol
- 4 § förordningen (2014:880) om sprängämnesprekursorer

Dynamisk hänvisning

- 3 kap. 7 § lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism

- 6 § lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster
- 3 § lagen (2023:704) om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post
- 5 § förordningen (2007:854) med instruktion för Försvarets materielverk
- 1 § förordningen (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering
- 11 § förordningen (2016:602) om finansiering av Post- och telestyrelsens verksamhet
- 3 § förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning
- 15 § fastighetsmäklarförordning (2021:518)
- 5 § och 7 § förordningen (2022:1286) om vissa förfaranden vid registrering av aktiebolag och filialer

Kostnadsuppskattning av eIDAS-förordningens bilaga VI

På uppdrag av Utredningen om säker
och tillgänglig digital identitet



2024-05-31

Wilhelm Hulfin, Hampuz Cederlind och Svante Eriksson



Innehållsförteckning

1.	Inledning.....	3
1.1.	BAKGRUND.....	3
1.2.	SYFTE OCH MÅL.....	4
1.3.	FRÅGESTÄLLNINGAR, GENOMFÖRANDE OCH AVGRÄNSNINGAR.....	4
1.4.	DISPOSITION.....	5
2.	Metod för kartläggning och beräkning.....	6
2.1.	METOD FÖR KARTLÄGGNING AV BERÖRDA AKTÖRER.....	6
2.2.	METOD FÖR ATT UPSKATTA KOSTNADER.....	7
3.	Identifiering av berörda aktörer.....	9
3.1.	ADRESS, ÅLDER, KÖN, CIVILSTÅND, FAMILJESAMMANSÄTTNING, NATIONALITET OCH MEDBORGARSKAP.....	9
3.2.	UTBILDNINGSKVALIFIKATIONER, TITLAR OCH LICENSER.....	9
3.3.	YRKESKVALIFIKATIONER, TITLAR OCH LICENSER.....	10
3.4.	BEFOGENHETER OCH MANDAT ATT FÖRETRÄDA FYSISK ELLER JURIDISK PERSON.....	11
3.5.	OFFENTLIGA TILLSTÅND OCH LICENSER.....	11
3.6.	FÖR JURIDISKA PERSONER, FINANS- OCH FÖRETAGSDATA.....	12
4.	Kostnadsberäkningar.....	13
4.1.	OSÄKERHETER.....	13
4.2.	FAKTISKA UPSKATTNINGAR FRÅN MYNDIGHETER.....	14
4.2.1.	Adress, ålder, kön, civilstånd, familjesammansättning, nationalitet och medborgarskap	14
4.2.2.	Utbildningskvalifikationer.....	14
4.2.3.	Befogenheter och mandat att företräda fysisk eller juridisk person.....	15
4.3.	BERÄKNADE UPSKATTNINGAR.....	16
4.3.1.	Berörda myndigheter.....	16
4.3.2.	Kommuner och länsstyrelser.....	17
4.4.	SAMLAD KOSTNADSUPPKATTNING.....	19
5.	Slutsatser.....	20
	Referenser.....	21
	Bilagor.....	22



1. Inledning

1.1. Bakgrund

Den 3 juni 2021 presenterade Europeiska kommissionen förslag till ändring av EU:s förordning om elektronisk identifiering för att fastställa en ram för en europeisk digital identitet (ändring av förordning 910/2014). Kommissionens förslag, som nu antagits, är att varje medlemsstat ska utfärda en europeisk så kallad digital identitetsplånbok. Med den digitala identitetsplånboken ska fysiska och juridiska personer på ett säkert sätt kunna begära, erhålla, lagra, välja, kombinera och använda personidentifieringsuppgifter och så kallade attributintyg (betyg, körkort, e-recept med mera) för autentisering online och offline samt skriva under med kvalificerade elektroniska underskrifter.

Regeringen har gett Utredningen om säker och tillgänglig digital identitet (I 2022:04) i uppdrag att analysera och föreslå förändringar som följer av den reviderade eIDAS-förordningen.¹ Detta ska utredningen redovisa i sitt slutbetänkande i maj 2024.

Förändringarna av eIDAS-förordningen kommer att innebära nya uppgifter och krav för offentlig sektor. Berörda myndigheter, kommuner med flera kommer att behöva utveckla digitala lösningar för att utge och hantera attributintyg samt säkerställa identitetshantering i enlighet med förslaget. Detta kommer leda till kostnader för berörda aktörer.

Enligt artikel 45e i eIDAS-förordningen ska medlemsstaterna säkerställa att attributintyg från "kvalificerade tillhandahållare av betrodda tjänster" på begäran av användaren kan verifieras elektroniskt mot den relevanta autentiska källan² eller via utsedda mellanhänder som erkänns på nationell nivå. I bilaga VI till eIDAS-förordningen fastställs vilka attribut som är ett minimum för varje medlemsland att tillhandahålla. De offentliga aktörer som ansvarar för register avseende exempelvis folkbokföring, utbildningskvalifikationer eller offentliga fillstånd och licenser kommer därmed behöva utveckla digitala lösningar för att tillhandahålla attributintyg själva eller utse någon som gör det åt dem, och validera attributintyg utfärdade av kvalificerade tillhandahållare av betrodda tjänster.

Som underlag för regeringens arbete med den reviderade eIDAS-förordningen har Utredningen om säker och tillgänglig digital identitet gett Governo AB i uppdrag att kartlägga vilka offentliga aktörer som berörs av kraven i bilaga VI av eIDAS-förordningen samt uppskatta kostnaden för att efterleva dessa.

¹ Europaparlamentets och rådets förordning (EU) 2024/1183 (2024)
https://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=OJ:L_202401183#a1e3705-1-1 (2024-05-29)

² Register/system som tillhandahåller attribut om en fysisk eller juridisk person och som anses vara en primär källa till denna information på nationell nivå.



1.2. Syfte och mål

Syftet med Governos uppdrag är tudelat:

- ✦ Kartlägga vilka offentliga aktörer som berörs av kravet i bilaga VI av eIDAS-förordningen.
- ✦ Uppskatta kostnader för berörda offentliga aktörer att utfärda attributintyg samt validera attributintyg utfärdade av kvalificerade tillhandahållare av betrodda tjänster.

Målet med uppdraget är att uppdragsgivaren efter genomfört arbete har fått en bra och välgrundad kartläggning samt analys av de aktuella frågeställningarna. Och att denna analys ger ett bra underlag för regeringens fortsatta arbete.

1.3. Frågeställningar, genomförande och avgränsningar

Följande frågeställningar har behandlats i uppdraget:

- ✦ Vilka svenska aktörer berörs av kravet i bilaga VI till eIDAS-förordningen – i den meningen att de har ansvar för de attributintyg varje medlemsland som ett minimum ska utfärda?
- ✦ Vilka kostnader – i uppbyggnadsskedet och löpande – medför den nya förordningen för berörda offentliga aktörer gällande utfärdande av attributintyg och validering av attributintyg utfärdade av kvalificerade tillhandahållare av betrodda tjänster?

Governos kartläggning av berörda aktörer baseras på information från internet samt intervjuer med diverse experter på olika myndigheter. Som underlag för Governos kostnadsberäkningar har ett flertal berörda myndigheter efter förfrågan från oss tillhandahållit egna kostnadsuppskattningar av hur de påverkas av förändringarna som följer eIDAS-förordningens bilaga VI. Dessa myndigheter har valts ut med stöd av vår kartläggning av berörda aktörer. En mer detaljerad genomgång av metoden bakom respektive delmoment framgår i kapitel 2.

Flera avgränsningar har gjorts i uppdraget, vilka har stämmts av med uppdragsgivaren. Kartläggningen av aktörer som berörs av kravet i eIDAS-förordningens bilaga VI behandlar enbart *offentliga* aktörer. För kostnadsberäkningarna gällande utfärdande och validering av attributintyg, har denna studie avgränsats till att i första hand fokusera på utfärdandeprocessen. Av osäkerhetsskäl behandlas inte validering av information från utlandet – att döma av vissa intervjuer kan sådana aktiviteter dock komma att utgöra en betydande kostnad i omställningen till bilaga VI. Det är dock en process som inte berörs i denna undersökning. Ytterligare avgränsningar presenteras löpande i texten.

Samtliga aktörer som berörs av kraven i bilaga VI är autentiska källor till den information som attributintyg utfärdas av. Det finns däremot ett steg mellan utfärdandet av attributintyg från den autentiska källan till den digitala plånboken, en slags överföringsmekanism, där det utfärdade attributintyget processas digitalt innan det skickas vidare till plånboken. En offentlig aktör som utgör autentisk källa till en viss typ av



information kan, men måste inte, också ansvara för denna överföring. Vilka myndigheter som kommer ha vilka roller med hänsyn till detta är i nuläget oklart och därför går kostnadsuppskattningen som presenteras i rapporten inte in på detta mer specifikt. Vissa myndigheter har däremot i sina uppskattningar de tillhandahållit oss avgränsat bort detta helt eller räknat på kostnader utifrån olika scenarier.

Inledningsvis bör poängteras att det i dagsläget råder stor osäkerhet gällande vad eIDAS-förordningen och bilaga VI kommer att innebära i mer detalj. Dessa osäkerheter är av både teknisk, organisatorisk och juridisk karaktär, till exempel finns det ännu ingen mer detaljerad genomförandeakt eller överenskommelse om hur offentliga aktörers efterlevande av kraven i bilaga VI kan koordineras. Genomgående under datainsamlingen har därför de aktörer som kontaktats för uppdraget vittnat om att de för närvarande har svårt att mer exakt bedöma hur omställningen till kraven ska ske mer praktiskt eller om man överhuvudtaget kommer bli påverkad.

Mot denna bakgrund bör resultaten som presenteras i denna rapport tolkas med försiktighet. Vår bedömning är dock att rapporten ger bästa möjliga svar på uppdragets frågeställningar givet de osäkerheter som föreligger.

1.4. Disposition

Bakgrund till det praktiska genomförandet, vald metod för kartläggningen av aktörer och beräkningarna redovisas i kapitel 2. Governos kartläggning av berörda aktörer redovisas i kapitel 3. Kapitel 4 presenterar uppskattade kostnader för utfärdande av attributintyg och kapitel 5 sammanfattar rapportens resultat.



2. Metod för kartläggning och beräkning

2.1. Metod för kartläggning av berörda aktörer

Grunden för kartläggningen av vilka aktörer som kommer beröras av kraven i bilaga VI har varit egen efterforskning i kombination med kvalitetssäkrande intervjuer. Under arbetets inledning hölls sonderande intervjuer med Myndigheten för digital förvaltning (DIGG), Bolagsverket och svenska universitetsdatanätverket (Sunet). Genom dessa möten var det möjligt att dels säkerställa att undersökningen hittar rätt berörda aktörer, dels bli hänvisad till källor där berörda aktörer för respektive attribut framgår. I tabell 1 redovisas hur berörda aktörer hittats för respektive attribut i bilaga VI.

Tabell 1: Källa för kartläggningens respektive delar

Attribut enligt bilaga VI	Källa
Adress	DIGG, egen efterforskning
Ålder	DIGG, egen efterforskning
Kön	DIGG, egen efterforskning
Civilstånd	DIGG, egen efterforskning
Familjesituation	DIGG, egen efterforskning
Nationalitet	DIGG, egen efterforskning
Utbildning, titlar och licenser	Sunet
Yrkeskvalifikationer, titlar och licenser	Universitets- och högskolerådets (UHR) lista över reglerade yrken, kvalitetssäkrad av Bolagsverket ³
Befogenheter och uppdrag att företräda fysiska eller juridiska personer	Bortavgränsad, utifrån underlag från Bolagsverket
Offentliga tillstånd och licenser	DIGG:s klassificering av statliga myndigheter 2022 ⁴
För juridiska personer, finansiella uppgifter och företagsuppgifter	Skatteverket, kvalitetssäkrad av Bolagsverket ⁵

³ Universitets- och högskolerådet (UHR). *Reglerade yrken* (2024) <https://www.uhr.se/bedomning-av-utlandsk-utbildning/arbete-och-studier/arbeta-i-sverige/Reglerade-yrken/> (2024-04-04)

⁴ DIGG. *Bilaga 2: Klassificering av statliga myndigheter 2022* (2023) <https://www.digg.se/download/18.5d519bdf18bdf9fbd001191a/1701168602278/Bilaga%202%20Klassificering%20av%20statliga%20myndigheter%202022.pdf> (2024-04-03)

⁵ Skatteverket. *Organisationsnummer* (u.å.) <https://skatteverket.se/foretag/drivaforetag/startaochregistrera/organisationsnummer.4.361dc8c15312eff6fd235d1.html> (2024-04-09)



Kartläggningens ambition har varit att identifiera vilka myndigheter som är ansvariga för de register över, och/eller är den autentiska källan till, den information som efterfrågas enligt bilaga VI. Resultatet av kartläggningen presenteras i kapitel 3. En redovisning för vilka problem som finns med att göra en kostnadsuppskattning gällande fullmakter återfinns i kapitel 4.

2.2. Metod för att uppskatta kostnader

Vår ambition har varit att, i den mån det är möjligt, efterfråga uppskattningar direkt från berörda myndigheter. Utifrån uppdragets omfattning och tidsram har det däremot inte varit möjligt att efterfråga uppskattningar från samtliga berörda myndigheter. För uppdragets genomförande har vi därför som arbetsätt valt att bara kontakta ett urval av de berörda myndigheterna. För att avgöra vilka som bör kontaktas har samtliga aktörer delats in i två grupper:

1. Offentliga aktörer med ett mer specifikt ansvar för ett särskilt/särskilda attributintyg. Kostnaderna denna grupp aktörer uppskattas behöva bära är mer unik och kan härledas till ett särskilt uppdrag och särskilda förutsättningar. Exempel på en sådan aktör är Skatteverket med ansvar för folkbokföringen. Samtliga aktörer i denna grupp har blivit kontaktade och tillfrågade om kostnadsuppskattningar.
2. Offentliga aktörer som enligt vår kartläggning bedöms ansvara för attributintyg som är mer generella och inte helt uppenbara i vad exakt de efterfrågar, exempelvis alla offentliga aktörer som utfärdar tillstånd. Från denna större mer generella grupp offentliga aktörer har ett urval kontaktats för uppskattningar. Kostnadsberäkningar från detta urval har sedan använts för att beräkna kostnaden för resterande offentliga aktörer i gruppen.

Efter inledande sonderande intervjuer framkom två faktorer som särskilt betydelsefulla för den kostnad som anpassning till den nya förordningen kommer innebära:

- ✦ myndighetens storlek
- ✦ myndighetens digitala mognad.

Urvalet av offentliga aktörer från den andra gruppen ovan i syfte att göra ytterligare beräknade uppskattningar har därmed gjorts med hänsyn till dessa faktorer. En myndighets storlek har betydelse i sammanhanget eftersom vi antar att den avspeglar hur efterfrågade myndighetens tjänster är. Vidare kommer digital mognad spela en viktig roll eftersom utfärdande och validering av attributintyg ställer krav på utveckling av tekniska lösningar. De berörda aktörernas respektive digitala mognad kan därför avgöra hur krävande denna tekniska anpassning blir för dem.

Hur ovanstående faktorer kan påverka den totala kostnaden kan också kompliceras ytterligare. En myndighets storlek kommer exempelvis inte bara påverka efterfrågan på tjänster utan sannolikt även myndighetens tillgång till tekniskt kunnig personal. Högre digital mognad behöver inte heller innebära lägre kostnader för att nå upp till kraven i bilaga VI. Om en myndighets tekniska infrastruktur visserligen är väl utvecklad men svår



att ansluta till den tekniska lösning som den digitala plånboken bygger på, kan det snarare utgöra ett hinder.

Trots ovanstående problematik kan dessa två faktorer förutsättas ge bäst grund för att under förutsättningarna göra ett urval. De har pekats ut som avgörande av flera av de myndigheter vi talat med och är i sammanhanget ett logiskt sätt att gruppera en varierad samling offentliga aktörer.

Myndigheternas storlek har vi valt att kategorisera utifrån deras antal årsarbetskrafter – baserat på data från Statskontoret avseende antalet årsarbetskrafter för 2023.⁶ Även om det är ett grovt mått, så är det en vanlig metod för att uppskatta en myndighets storlek.⁷

Det är svårare att hitta ett mått på digital mognad, dels för att det är ett mer komplicerat begrepp, dels för att det finns mindre data på området. DIGG genomför dock sedan ett antal år tillbaka en årlig enkätundersökning som syftar till att förstå myndigheters digitala mognad. Enkäten resulterar i fyra index varav vi har valt att använda ett som stöd för att uppskatta digital mognad. Mer information om respektive index och vilka frågor som ingår i dessa framgår i bilaga 2.

Utifrån ovanstående har berörda myndigheter kategoriserats. Det visar sig då att en myndighets storlek och digital mognad i allmänhet följer varandra ganska tätt – även om det också finns undantag. Utifrån detta gjorde vi ett urval av myndigheter som därefter blev tillfrågade om kostnadsuppskattningar. De kostnadsuppskattningar som inkommit har sedan använts för att uppskatta kostnaden för de övriga offentliga aktörerna. Resultatet av kostnadsuppskattningarna och den sammanlagda kostnaden redovisas i kapitel 4.

⁶ Statskontoret, *Myndigheternas storlek* (u.å.) <https://www.statskontoret.se/fokusomraden/fakta-om-statsforvaltningen/myndigheternas-storlek/> (2024-04-09)

⁷ DIGG, *Digitalisering för förvaltningsgemensam nytta*. (2023) <https://www.digg.se/analys-och-uppfoljning/publikationer/publikationer/2023-09-06-digitalisering-for-forvaltningsgemensam-nytta> (2024-04-10)



3. Identifiering av berörda aktörer

I detta kapitel ges en översiktlig redovisning av resultatet av vår kartläggning av berörda aktörer. Se även bilaga 1 där kartläggningen återges i Excel-format. I kartläggningen som presenteras i kapitlet redogörs för vilken information som framgår från källorna som redovisas i tabell 1, vilka myndigheter som kan tänkas beröras när bilaga VI praktiskt implementeras diskuteras också.

Inledningsvis bör dock påpekas att det fortfarande finns osäkerheter kring berörda aktörer – även om vi, som framgår i avsnitt 2.2, har vidtagit flera åtgärder för att kvalitetssäkra kartläggningen. Osäkerheterna är av både teknisk och juridisk art, bland annat på grund av att det ännu saknas en genomförandeakt.

3.1. Adress, ålder, kön, civilstånd, familjesammansättning, nationalitet och medborgarskap

Flera delar av informationen som efterfrågas i bilaga VI återfinns i folkbokföringen, för vilken Skatteverket är ansvarig.⁸ I samtal med oss har företrädare för myndigheten bekräftat att de träffas av kraven med hänsyn till den efterfrågade informationen.

3.2. Utbildningskvalifikationer, titlar och licenser

Relevanta attributintyg av utbildningskvalifikationer definieras som bevis på en genomförd utbildning. Det behöver inte nödvändigtvis vara en examen i sig utan kan även vara en kurs genomförd på en högskola. Informationen som träffas av denna del av bilaga VI kan delas in i tre grupper:

- ✦ grundskoleutbildning,
- ✦ eftergymnasial högskoleutbildning, samt
- ✦ yrkesutbildning.

Grundskoleutbildning delas in i två delar, grundskolan och gymnasiet. Den autentiska källan för såväl grundskole- som gymnasieresultat finns hos den enskilda kommunen. Vad gäller studieresultat från gymnasiet är vår bedömning dock att dessa med fördel skulle kunna samlas in hos Universitets- och högskolerådet (UHR) via den nationella betygsdatabasen (Beda).⁹ Den bild vi fått under arbetets gång är att det förs diskussioner om att UHR i framtiden kan få ett uppdrag att tillhandahålla relevanta attributintyg med hänsyn till gymnasiet. Något beslut i sådan riktning föreligger dock inte i dagsläget och UHR har inget sådant uppdrag idag.

⁸ Skatteverket, *Folkbokföringsdatabasen*, (u.å.)
<https://skatteverket.se/privat/folkbokforing/attvarafolkbokford/folkbokforingsdatabasen.4.3810a01c150939e893f16fe2.html> [2024-04-09]

⁹ Universitets- och högskolerådet, *Beda – nationella betygsdatabasen*, (2021)
<https://www.uhr.se/systemtjanster-for-larosaten/stodsystem-for-larosaten/betygsdatabasen-beda/> [2024-05-02]



Uppgifter om eftergymnasial högskoleutbildning finns hos enskilda lärosäten. Det är dock troligt att Ladokkonsortiet kommer få ett ansvar att utfärda attributintyg för anslutna lärosäten. Detta har representanter från Ladok själva bekräftat i våra kontakter med dem.

Utbildningskvalifikationer från yrkeshögskolor finns inte samlade på en plats och det finns inte heller en aktör som har i uppdrag att samla in denna information. Däremot har det i utredningen om Framtidens yrkeshögskola (SOU 2023:31) föreslagits att Myndigheten för Yrkeshögskolan (MYH) ska få i uppdrag att göra en förstudie om ett förstärkt system för studiedokumentation. Om MYH skulle få ett utökat ansvar att utveckla ett utbyggt studiesystem är det också tänkbart att de, som ett nästa steg, kan få i uppdrag att utfärda attributintyg med hänsyn till denna information.

3.3. Yrkeskvalifikationer, titlar och licenser

En rimlig bild av vilka yrkeskvalifikationer som kan vara relevanta utifrån denna del av bilaga VI ges av en lista över reglerade yrken som UHR redovisar på sin webbplats.¹⁰ Med reglerade yrken avses sådana där det enligt svensk lag krävs någon form av legitimation, behörighet eller liknande för att få utöva yrket i fråga.

Sammanlagt identifierar UHR 15 huvudsakliga aktörer, exklusive samtliga länsstyrelser, som utfärdar kvalifikationer för ett flertal olika yrkesgrupper. De berörda myndigheterna som framkommit genom denna undersökning är:

- ✦ Arbetsmiljöverket
- ✦ Boverket
- ✦ Elsäkerhetsverket
- ✦ Fastighetsmäklarinspektionen
- ✦ Finansinspektionen
- ✦ Folkhälsomyndigheten
- ✦ Jordbruksverket
- ✦ Kammarkollegiet
- ✦ Myndigheten för samhällsskydd och beredskap
- ✦ Patentombudsnamnden
- ✦ Revisorsinspektionen
- ✦ Skolverket
- ✦ Socialstyrelsen
- ✦ Transportstyrelsen
- ✦ Universitets- och högskolerådet

Utöver dessa finns även reglerade yrken inom polisen, försvaret och rättsväsendet. Gällande yrkeskvalifikationer inom Polismyndigheten och Försvarsmakten kommer dessa sannolikt inte omfattas av kraven i bilaga VI, på grund av särskilda bestämmelser kring uppgifter om nationell säkerhet. Detta behöver dock utredas vidare. Vad gäller yrkeskvalifikationer inom rättsväsendet är bilden mer otydlig. Vi har varit i kontakt med

¹⁰ Universitets- och högskolerådet. *Reglerade yrken*. (2024) <https://www.uhr.se/bedomning-av-utlandsk-utbildning/arbeta-och-studier/arbeta-i-sverige/Reglerade-yrken/> (2024-04-04)



Domstolsverket som bedömer att de inte kommer beröras av kraven i bilaga VI gällande yrkeskvalifikationer. Ett problem som har lyfts gällande detta är att varje domstol självständigt beslutar om tillsättandet av tjänster, exempelvis som domare av olika slag. Det är därmed inte givet att det för sådana yrkeskvalifikationer finns ett samlat register som omfattar den information som efterfrågas i bilaga VI. Exakt hur rättsväsendet kommer påverkas är fortfarande oklart, frågan har därmed avgränsats bort i samråd med uppdragsgivaren.

3.4. Befogenheter och mandat att företräda fysisk eller juridisk person

Gällande befogenheter och mandat att företräda fysisk eller juridisk person, olika typer av fullmakter, ansvarar Bolagsverket idag för tjänsten Minaombud.se som gör det möjligt att företräda en annan part med hjälp av en digital fullmakt. Denna tjänst kommer troligtvis, enligt Bolagsverket, vara den tekniska grunden för utfärdande och validering av attributintyg gällande fullmakter. Bolagsverket menar vidare att alla offentliga aktörer kommer beröras av detta krav i bilaga VI, eftersom samtliga måste ansluta sig till Minaobud.se för att systemet ska fungera.

3.5. Offentliga tillstånd och licenser

Kartläggningen har identifierat cirka 30 aktörer som träffas av kraven i bilaga VI gällande tillstånd och licenser. Till dessa bör därtill även enskilda kommuner och länsstyrelser räknas med.

Grunden för denna kartläggning är DIGG:s klassificering av statliga myndigheter, en bilaga till DIGG:s uppföljning av statliga myndigheters digitalisering 2022.¹¹ Samtliga myndigheter som besvarat DIGG:s enkäter gällande åren 2020, 2021 och 2022 ingår i klassificeringen. Enkäterna skickas ut till ett urval av de statliga myndigheterna under regeringen samt till Riksrevisionen. I urvalet inkluderar DIGG endast myndigheter med mer än nio årsarbetskrafter och gör även vissa andra avgränsningar.¹² Totalt har 168 offentliga aktörer svarat med lite variation beroende på år. Våra kontakter med DIGG:s analysavdelning, som genomför enkätundersökningen, talar för att nästan samtliga myndigheter med tillståndsverksamhet bör vara inkluderade i DIGG:s undersökning. Eventuellt kan det dock finnas enstaka myndigheter med tillståndverksamhet som inte ingår i DIGG:s undersökning på grund av att de inte besvarat enkäten, samt kriterierna för urvalet.¹³ De identifierade aktörerna redovisas nedan:

¹¹ DIGG. *Bilaga 2: Klassificering av statliga myndigheter 2022 (2023)*
<https://www.digg.se/download/18.5d519baf18baf91bd001191a/1701168602278/Bilaga%20%20%20Klassificering%20av%20statliga%20myndigheter%202022.pdf> (2024-04-03)

¹² I DIGG:s enkät ingår bland annat inte Regeringskansliet, myndigheter under Försvarsdepartementet (fll exempel Fortifikationsverket och Försvarshögskolan) och heller inte SÄPO, Valmyndigheten, AP-fonderna, domstolarna och hyresnämnderna. För länsstyrelserna lämnas ett gemensamt svar för samtliga 21.

¹³ Enligt DIGG:s klassificering bedriver Naturvårdsverket inte tillståndsverksamhet. Vår efterforskning pekar däremot på att myndigheten visst utfärdar vissa tillstånd. Detta kan potentiellt förklaras av att gränsen mellan tillsyn- och tillståndsverksamhet inte är självklar inom vissa områden.



- ✦ Bolagsverket
- ✦ E-hälsomyndigheten
- ✦ Energimarknadsinspektionen
- ✦ Etikprövningsmyndigheten
- ✦ Exportkreditnämnden
- ✦ Fastighetsmäklarinspektionen
- ✦ Finansinspektionen
- ✦ Inspektionen för vård och omsorg
- ✦ Kemikalieinspektionen
- ✦ Kommerskollegium
- ✦ Lantmäteriet
- ✦ Migrationsverket
- ✦ Myndigheten för press, radio och tv
- ✦ Patent- och registreringsverket
- ✦ Polismyndigheten
- ✦ Post- och telestyrelsen
- ✦ Revisorsinspektionen
- ✦ Rymdstyrelsen
- ✦ Skatteverket
- ✦ Skolinspektionen
- ✦ Skolverket
- ✦ Socialstyrelsen
- ✦ Sveriges geologiska undersökning
- ✦ Statens medieråd (ingår sedan den 1 januari 2024 i Mediemyndigheten)
- ✦ Trafikverket
- ✦ Transportstyrelsen
- ✦ Universitets- och högskolerådet

3.6. För juridiska personer, finans- och företagsdata

Enligt nuvarande förslag ska Bolagsverket vara sammanhållande för LPID utfärdande-processen för Sverige. Attributintyg av finans- och företagsdata för juridiska personer berör däremot också, enligt Bolagsverket, myndigheterna som tillhandahåller information om organisationsnummer som preciseras av Skatteverket.¹⁴

Kartläggningen som gjorts indikerar att sammanlagt sju olika aktörer kommer att påverkas. Utöver Bolagsverket är de aktörer som ska tillhandahålla den största delen information Skatteverket samt Statistiska centralbyrån (SCB). Där till har även Kammarkollegiet, Lantmäteriet, respektive länsstyrelse samt Inspektionen för arbetslöshetsförsäkring identifierats som andra aktörer som kan beröras.

¹⁴ Skatteverket. *Organisationsnummer*. (u.å.)
<https://skatteverket.se/foretag/drivforetag/startaochregistrera/organisationsnummer.4361dc8c15312eff6fd235d1.html> (2024-04-09)



4. Kostnadsberäkningar

I detta kapitel redovisas vår uppskattning av vilka kostnader den nya förordningens bilaga VI medför för berörda offentliga aktörer med avseende på utfärdande av attributintyg och validering av attributintyg utfärdade av kvalificerade tillhandahållare av betrodda tjänster. Först behandlas vissa osäkerheter som påverkat beräkningarna, inklusive en kort sammanfattning om varför de aktörer som inte inkommit med uppskattningar avstod från att göra det. Därefter presenteras vår kostnadsuppskattning för samtliga aktörer identifierade som berörda i kapitel 3. Som avsnitt 2.2 tydliggör i mer detalj delar vi in samtliga berörda aktörer i två grupper beroende på deras roll med hänsyn till bilaga VIs genomförande. Denna gruppindelning speglar också hur vi redovisar framtagna kostnadsuppskattningar.

4.1. Osäkerheter

Vår bild är att de offentliga aktörer som tillfrågades om kostnadsuppskattningar för denna studie över lag har utrett frågan grundligt. Låt vara att vissa av de tillfrågade aktörerna inte lyckades leverera det efterfrågade underlaget. Ett mervärde som därmed skapats i och med detta arbete är att syftet med Utredningen om säker och tillgänglig digital identitet har uppmärksamats inom den offentliga sfären och flera myndigheter och offentliga aktörer har därmed börjat reflektera kring vad som kommer att krävas av dem för att efterleva kraven som ställs i bilaga VI och eIDAS-förordningen över lag.

Som tidigare nämnts har samtliga kontaktade aktörer lyft att deras kostnadsuppskattningar, som redovisas i detta kapitel, är osäkra och bör läsas med försiktighet. Vissa bedömde att osäkerheten är så pass stor att de valde att inte inkomma med någon kostnadsuppskattning. Samtliga kostnadsuppskattningar och förklaringar till varför man avstått från att göra en kostnadsuppskattning återfinns i rapportens bilagor. Här vill vi dock översiktligt redogöra för hur de aktörer som avstått har resonerat.

En av dessa aktörer är UHR som meddelade att de avstår från att genomföra en kostnadsberäkning då myndigheten inte anser att den kan leverera ett reellt och användbart estimat. Skälen för detta är i huvudsak att UHR inte utfärdar gymnasiala meriter och därmed inte är primärkällan för den data som finns i Beda. Utöver detta är överföring av gymnasiala meriter till Beda inte obligatorisk för samtliga aktörer som behöver leverera data till Beda. UHR bedömer inte heller att Beda innehåller samtliga attribut som behövs för att kunna leverera attributintyg. UHR kommer följaktligen till slutsatsen att det behöver genomföras en mer utförlig teknisk och juridisk utredning för att se över förutsättningarna för Beda att användas i detta syfte.

Vidare avstod Kemikalieinspektionen från att göra en kostnadsberäkning eftersom de, enligt egen bedömning, inte omfattas av kraven som ställs i bilaga VI till skillnad från den slutsats som presenteras i rapportens kapitel 3. Anledningen till detta är att de utfärdar produktgodkännanden för en produkt att få finnas på marknaden och inte



tillstånd för huruvida företag ska få tillstånd att bedriva viss verksamhet. Myndigheten menar alltså att de inte ser att det skulle finnas ett behov för någon att kunna visa upp ett beslut om ett sådant produktgodkännande i original. Detta är ett intressant resonemang som också visar hur det i dagsläget går att göra olika bedömningar kring vad bilaga VI efterfrågar och innebär mer konkret.

Vidare har inte heller SCB, SKR, eller länsstyrelserna (i det senare fallet via länsstyrelsernas gemensamma stödfunktion för informationssäkerhet och dataskydd) inkommit med uppskattningar. SCB menar att de måste utreda frågan vidare och att de därför i nuläget inte kan ge en kostnadsestimering. Även SKR och länsstyrelserna uppger att de inte haft möjlighet att uppskatta kostnader under rådande omständigheter.

4.2. Faktiska uppskattningar från myndigheter

I detta avsnitt presenteras kostnadsuppskattningar för adress, ålder, kön, civilstånd, familjesammansättning, nationalitet och medborgarskap; utbildningskvalifikation; samt i den utsträckning det är möjligt, befogenheter och mandat att företräda fysisk eller juridisk person. Samtliga kostnader som redovisas bygger, i den mån det är möjligt, på beräkningar direkt från den berörda myndigheten.

4.2.1. Adress, ålder, kön, civilstånd, familjesammansättning, nationalitet och medborgarskap

Enligt Skatteverket som kommer att ha ansvaret för dessa attribut bedöms anpassning av stödjande tekniska tjänster kosta mellan 10 och 15 miljoner kronor. Utveckling inom folkbokföringen bedöms kosta ytterligare 10 miljoner kronor men är, enligt myndighetens företrädare, ett särskilt grovt estimat. Alltså bedöms de totala utvecklingskostnaderna bli mellan 20 och 25 miljoner kronor. Till detta tillkommer en löpande förvaltningskostnad på 8 till 10 miljoner kronor per år.

4.2.2. Utbildningskvalifikationer

Detta avsnitt följer den gruppindelning som presenterades i kapitel 3, det vill säga grundskoleutbildning (inklusive både grundskola och gymnasium), eftergymnasial högskoleutbildning samt yrkesutbildning.

För högre utbildning har Ladok identifierats som den aktören med ett övergripande ansvar. Ladokkonsortiet deltar i ett av de EU-finansierade LSP (Large Scale Pilot) om EUDI wallet, nämligen DC4EU (Digital Credentials for Europe). Detta bedöms ha en stor inverkan på kostnadsberäkningen eftersom de utgår från att stora delar av utvecklingen kommer att ske inom projektet och att Ladok kommer kunna utnyttja hela utvecklingsresultatet utan kostnad. Ladokkonsortiets insats i projektet är därmed att skapa möjlighet att föra över meriter från högre utbildning till plånboken. Det bör noteras att det som görs av konsortiet görs tillgängligt för alla medlemmar i konsortiet så i princip hela sektorn för högre utbildning kommer kunna utnyttja resultatet utan



särkostnad. För att göra detta uppskattas en utvecklingskostnad på 3,5 miljoner kronor och en ytterligare årlig förvaltningskostnad på 3 miljoner kronor.

Vad gäller grundskolan försvåras våra möjligheter att beräkna kostnaden av att Sveriges Kommuner och Regioner (SKR) inte inkommit med en uppskattning. På grund av detta kommer kostnaden för kommunerna i stället uppskattas separat i kommande avsnitt, tillsammans med övriga kostnader som kommunerna troligtvis kommer behöva bära i och med bilaga VI.

Även för gymnasiet har vi motsvarande problem i och med att UHR inte inkommit med någon uppskattning. Om UHR skulle få detta uppdrag är det tänkbart att deras kostnader kommer vara högre än Ladoks som har en, för sammanhanget, mer utvecklad teknisk infrastruktur att använda. En uppskattning som skulle ta höjd för de osäkerheter som finns är att multiplicera Ladoks uppskattning med två. Då skulle UHR:s utvecklingskostnad bli 7 miljoner kronor och förvaltningskostnaden 6 miljoner kronor per år. Det estimatet är dock högst osäkert och är Governos egen uppskattning.

Avslutningsvis för yrkesutbildningar menar MYH att förutsättningarna för att göra en kostnads kalkyl är väldigt vaga. Tidigare utvecklingsprojekt som påminner i omfattning och som myndigheten genomfört har krävt mellan 1000 och 2000 timmars arbete. Som ett tillägg till detta behöver myndigheten utveckla ett förstärkt system för studiedokumentation som uppskattas tillföra ytterligare cirka 1000 arbetstimmar. En kostnadsuppskattning för detta är mellan 1 och 3 miljoner kronor med en årlig förvaltningskostnad om 20 procent av utvecklingskostnaden, det vill säga mellan 200 000 och 600 000 kronor per år.

4.2.3. Befogenheter och mandat att företräda fysisk eller juridisk person

För att förstå kostnader kopplade till utfärdande av fullmakter har Bolagsverket tillfrågats i egenskap av expert och förvaltare av Minaombud.se som, enligt Bolagsverket, högst sannolikt kommer utgöra den tekniska grunden för dessa attributintyg. Bolagsverket menar däremot att det i dagsläget inte är möjligt att beräkna kostnader för utfärdande av allmänna fullmakter av två huvudsakliga skäl:

- ✦ För det första kommer samtliga offentliga aktörer enskilt behöva ansluta till den tekniska infrastruktur som finns. Förutsättningarna för detta kan variera stort mellan aktörer vilket Bolagsverket menar försvårar en eventuell kostnadsuppskattning.
- ✦ För det andra finns juridiska frågor som behöver utredas vidare. Ifall Minaombud.se ska vara stommen för detta projekt behöver dess legala grund ses över. Det kan kräva tekniska anpassningar i tjänsten och därmed ytterligare kostnader.

Allmänna fullmakter av ovan nämnt slag kommer utgöra den stora kostnadsposten vad gäller dessa attributintyg. Enligt Bolagsverket kan det däremot tillkomma ytterligare typer av attributintyg från denna del av bilaga VI, ett av dessa är "EU Power of Attorney". Bolagsverket vet redan i dagsläget att de kommer behöva hantera dessa attributintyg och har därmed inkommit med en kostnadsuppskattning för dess genomförande. Uppskattningen bygger på två olika scenarier beroende på huruvida de själva eller annan myndighet äger och driver Minaombud.se. I båda scenarier uppskattas kostnaden bli mellan 5 och 10 miljoner kronor. Det som skiljer dessa scenarier



åt är vad som kommer utgöra kostnaden. Bolagsverket menar därtill att förutsättningarna för att beräkna kostnader gällande fullmakter är så pass osäkra att de i dagsläget inte kan uppskatta en årlig förvaltningskostnad.

Bolagsverket har särskild kunskap på området och har bistått oss i egenskap av att vara en expertmyndighet. På grund av deras särskilda kompetens och speciella förutsättningar har vi bedömt att det inte är lämpligt att använda deras uppskattning för att beräkna andra myndigheters kostnader. Därför presenterar vi här, och inte i kommande avsnitt, deras kostnad för utfärdande av övriga attributintyg. Enligt myndigheten kommer de, som nämnades i kapitel 3, få ett ansvar för LPID (organisationsidentiteter) och attesteringar som ska utfärdas på ett samlat sätt via Bolagsverket. Denna grundläggande infrastruktur beräknas kosta 15 miljoner kronor att utveckla och 6 miljoner kronor årligen i förvaltningskostnader. Denna uppskattning täcker inte kostnad för andra myndigheter att tillhandahålla organisationsinformation till myndigheten. Utöver detta kommer Bolagsverket, som också beskrivs i kapitel 3, behöva utfärda flera andra olika attributintyg specificerade i bilaga VI. Utvecklingskostnaden för dessa uppskattas vara 14 miljoner kronor och förvaltningskostnaden 8 miljoner kronor per år. Sammanlagt kommer myndigheten behöva bära 29 miljoner kronor i utvecklingskostnad och 14 miljoner kronor per år i löpande förvaltningskostnader utöver kostnader för "EU Power of Attorney".

4.3. Beräknade uppskattningar

Här presenteras kostnadsuppskattningar för attributintyg gällande yrkeskvalifikationer, titlar och licenser; offentliga tillstånd och licenser samt för juridiska personer, finans och företagsdata. Skillnaden med detta avsnitt kontra 4.2 är att betydligt fler aktörer berörs av kraven för utfärdande av dessa attributintyg. Sammanlagt har kostnadsuppskattningar från fem olika myndigheter inkommit som använts för att göra nedanstående beräkningar. På grund av att varken SKR eller länsstyrelserna inkommit med kostnadsuppskattningar genomförs en samlad uppskattning för dem också. Denna redovisas separat från uppskattningen vi beräknar för berörda myndigheter.

4.3.1. Berörda myndigheter

Som utgångspunkt för vår beräkning i denna del har vi antagit att de tekniska lösningar som kommer att krävas för att utfärda de berörda attributintygen kommer att vara tämligen likartad för samtliga berörda myndigheter. Vi har därför valt att betrakta myndigheterna som en samlad grupp. Eftersom vi inte haft möjlighet att samla in uppskattningar från samtliga dessa myndigheter har det också varit nödvändigt att göra en egen beräknad uppskattning. För att genomföra uppskattningen delades samtliga berörda aktörer in i fem olika grupper utifrån årsarbetskrafter och matchades därefter med en liknande myndighet som inkommit med en kostnadsuppskattning.



Tabell 2: Kostnadsuppskattningar per gruppindelning i miljoner kronor

Antal årsarbetskrafter	Antal myndigheter i grupp	Myndighet vars uppskattning bildat grund	Uppskattad utvecklingskostnad	Uppskattad årlig förvaltningskostnad
0 – 100	10	Revisorsinspektionen	1-5	0,2-1*
100 – 500	11	Post- och telestyrelsen	7,5-14	2
500 – 760	4	Finansinspektionen	17	8,5
760 – 2000	6	Socialstyrelsen	65	13
2000 –	3	Transportstyrelsen	81	16,2
Summa	34		793,5-905	184,6-192,6

*Revisorsinspektionen kunde inte uppskatta en förvaltningskostnad själva. I stället har vi, med inspiration från de andra uppskattningarna, estimerat den till 20 procent av utvecklingskostnaden.

Som tabell 2 visar kan den ekonomiska kostnaden uppskattas till två olika summor genom att räkna på både den lägre och högre kostnaden för de vars kostnadsuppskattningar innehåller ett spann.

Sent i arbetet blev vi uppmärksammade på att även Försäkringskassan troligtvis kommer bli träffade av bilaga VI genom myndighetens ansvar att för svensk del utfärda det europeiska sjukförsäkringskortet – även om detta kort möjligen inte är att betrakta som ett tillstånd av det slag vi utgått från i kartläggningen i kapitel 3. Om Försäkringskassan läggs till ovanstående sammanställning så ökar summorna förhållandevis mycket – med hänsyn till Försäkringskassans storlek har vi då använt Transportstyrelsens kostnadsuppskattning som riktmärke. Inklusivt Försäkringskassan blir därmed den samlade uppskattade utvecklingskostnaden 874,5 eller 986 miljoner kronor beroende på om det lägre eller högre spannet används. Den tillhörande årliga förvaltningskostnaden blir antingen 200,8 eller 208,8 miljoner kronor.

4.3.2. Kommuner och länsstyrelser

Som framgår i kapitel 3 uppskattas kommunerna träffas av kraven i bilaga VI vad gäller offentliga tillstånd och licenser och även potentiellt utbildningskvalifikationer för grundskolan. Länsstyrelserna träffas också med hänsyn till offentliga tillstånd men även gällande vissa yrkeskvalifikationer och finans- och företagsdata för vissa juridiska personer. Vi har gjort en grov kostnadsuppskattning för dessa aktörer, men beräkningsförutsättningarna försvarades av att varken SKR eller länsstyrelserna inkom med några uppskattningar.

Av de fem myndigheter som ovan i tabell 2 använts som riktmärke för att generalisera bedömer vi att Finansinspektionens kostnadsuppskattning är mest relevant att utgå från



avseende kommunerna. Kartläggningen visar att kommunerna, i likhet med Finansinspektionen, kommer att behöva utfärda två olika typer av attributintyg. Låt vara att karaktären på respektive aktörs attributintyg skiljer sig åt. Det måste också vägas in att kommunerna varierar mycket i storlek sinsemellan, vilket sannolikt lär påverka den totala kostnaden. Vi har därför antagit att Finansinspektionens kostnad enligt tabell 2 motsvarar kostnaden för större kommuner (över 70 000 invånare), och att resterande kommuners kostnad i fallande grad kan uppskattas som en procentandel av de stora kommunernas kostnad. Uppgifter om respektive kommuns invånarantal framgår nedan, tillsammans med en uppskattad kostnad.¹⁵

Tabell 3: Kostnadsuppskattning för kommuner viktad för invånarantal, miljoner kronor

Kommunstorlek (invånare)	Antal kommuner	Vikt	Utvecklingskostnad*	Förvaltningskostnad*
0 – 10000	74	0,25	314,5	157,25
10 – 30000	128	0,5	1088	544
30 – 70000	54	0,75	688,5	344,25
70000 –	34	1	578	289
Summa	290		2669	1334,5

*Normal utvecklingskostnad utifrån Finansinspektionens uppskattning är 17 miljoner kronor, förvaltningskostnaden 8,5 miljoner kronor.

Enligt uppskattningen som redovisas i tabell 3 uppgår den totala kostnaden för kommunerna till nästan 2,7 miljarder kronor och den årliga förvaltningskostnaden till cirka 1,3 miljarder kronor. Denna uppskattning vilar på antagandet att varje kommun utfärdar attributintygen självständigt och ej koordinerat av en central aktör. Skulle processen koordineras skulle kostnaden troligtvis bli lägre.

Länsstyrelsernas IT-funktion är centraliserad och därmed kan kostnaden för dessa aktörer också antas bli mindre än för kommunerna. Vi bedömer att Transportstyrelsens kostnadsberäkning enligt tabell 2 i detta fall är mer relevant att utgå från. I likhet med länsstyrelserna kommer Transportstyrelsen få ansvar för att utfärda flera olika attributintyg. Därtill har Transportstyrelsen verksamhet på olika orter. Sammanlagt finns 21 länsstyrelser medan Transportstyrelsen finns på 12 orter.¹⁶ Då Transportstyrelsens lokala kontor ungefär motsvarar hälften av antalet länsstyrelser skulle approximativt kunna antas att länsstyrelsernas kostnad blir minst dubbel så stor som Transportstyrelsens. Dock är antalet årsarbetskrafter på länsstyrelserna gemensamt närmare tre gånger så många som på Transportstyrelsen. Vid en sammanvägd bedömning uppskattar vi länsstyrelsernas utvecklingskostnad till 162 miljoner kronor och deras årliga förvaltningskostnader till 32,4 miljoner kronor.

¹⁵ Wikipedia. Lista över Sveriges kommuner. (u.å.) https://sv.wikipedia.org/wiki/Lista_%C3%B6ver_Sveriges_kommuner (2024-05-02)

¹⁶ Transportstyrelsen. Organisation. (2024) <https://www.transportstyrelsen.se/sv/om-transportstyrelsen/organisation/> (2024-05-02)



4.4. Samlad kostnadsuppskattning

I tabell 4 nedan sammanfattas de kostnadsuppskattningar som redovisats ovan. Uppskattningen presenteras som ett spann. Detta då flera tillfrågade offentliga aktörer gett sin kostnadsuppskattning i termer av en lägre och en högre kostnad.

Tabell 4: Samlad kostnadsuppskattning, miljoner kronor

Attribut	Uppskattning	Engångvis utvecklingskostnad	Årlig förvaltningskostnad
Adress, ålder, kön, civilstånd, familjesammansättning, nationalitet och medborgarskap	Skatteverket	20-25	8-10
Utbildningskvalifikationer, titlar och licenser	Ladok	3,5	3
	UHR	7	6
	MYH	1-3	0,2-0,6
Befogenheter och mandat att företräda fysisk eller juridisk person	Bolagsverket	5-10	
Yrkeskvalifikationer, titlar och licenser; offentliga tillstånd och licenser; samt för juridiska personer, finans och företagsdata	Beräkning, berörda myndigheter	874,5-986	200,8-208,8
	Beräkning, kommuner	2669	1334,5
	Beräkning, länsstyrelser	162	32,4
	Bolagsverket*	29	14
Summa		3771-3894,5	1598,9-1609,3

*Bolagsverkets uppskattning innehåller kostnad både för utfärdande av attributintyg myndigheten kommer ansvara för samt upprättande av LPID infrastruktur.



5. Slutsatser

I föregående kapitel redovisades vår uppskattning av vilka kostnader den nya förordningens bilaga VI medför för berörda offentliga aktörer med avseende på utfärdande av attributintyg och validering av attributintyg utfärdade av kvalificerade tillhandahållare av betrodda tjänster. Som framgår av tabell 4 bedömer vi att berörda aktörers engångsvisa utvecklingskostnad kommer att ligga på cirka 3,8 till 3,9 miljarder kronor och deras årliga förvaltningskostnader på cirka 1,6 miljarder kronor.

Som vi flera gånger betonat i rapporten ska den samlade kostnadsuppskattning som presenteras här tolkas med försiktighet. Detta då det finns flera osäkerheter på området. Osäkerheterna handlar bland annat om att det finns flera olika juridiska, organisatoriska och tekniska frågor som behöver utredas vidare innan det går att slutgiltigt slå fast vad bilaga VI kommer innebära mer konkret. Detta har också påverkat pålitligheten i de uppskattningar som vi fått från identifierade berörda myndigheter som sedan varit underlag för vidare uppskattningar i denna studie.

Till detta ska läggas att vi givet uppdragets ramar inte haft möjlighet att inhämta information om varje berörd aktörs egna specifika förutsättningar eller deras exakta ansvar med hänsyn till bilaga VI, utan har behövt bygga beräkningarna på antaganden om generaliserbarhet utifrån ett mindre antal fall. Den valda metoden innebär givetvis en risk för felkällor, även om den – det bör understrykas – enligt vår mening var den mest praktiskt tillämpbara i detta uppdrag.

Med dessa reservationer menar vi ändå att uppskattningen som presenteras är så heltäckande och exakt som det är möjligt att bli givet rådande förutsättningar och omständigheter. I jämförelse med andra studier som försökt uppskatta kostnaden av att digitalisera inom olika områden ter sig heller inte siffran som presenteras orrealistisk. Ett exempel är en rapport från Institutet för framtidsstudier enligt vilken det under en två- till femårsperiod kan kosta 70 till 100 miljarder kronor årligen att digitalisera kommunerna.¹⁷ Ett annat exempel är att SKR uppskattat att det kan kosta cirka 14 miljarder att digitalisera socialtjänsten.¹⁸ Detta indikerar snarare att kostnaden som uppskattats i denna rapport riskerar att ligga i underkant.

Avslutningsvis bör det poängteras att kostnadsuppskattningen som presenteras här inte täcker Försvarsmakten, Polismyndigheten eller rättsväsendet. Huruvida de träffas av kraven i bilaga VI och hur deras förutsättningar ser ut att möta dessa, givet särskilda bestämmelser om sekretess och nationell säkerhet, behöver utredas vidare. Deras speciella uppdrag och omständigheter kan tillföra ytterligare kostnader som denna studie och dess metod inte tar höjd för.

¹⁷ Anders Ekholm, Karim Jebari och Drasko Markovic, *Förbjuden framtid? Den digitala kommunen* (Institutet för Framtidsstudier 2018) <https://www.ifs.se/publikationer/ovrigt/forbjuden-framtid/>

¹⁸ Sveriges kommuner och regioner, *Vad kommer det att kosta socialtjänsten att investera i digitala lösningar?* (2024) <https://skr.se/skr/integrationsocialomsorg/socialomsorg/digitaliseringinomsocialtjansten/verkytgoochutveckling-sarbeten/kostnaderdigitaliseringsocialtjansten.32340.html> (2024-05-09)



Referenser

- DIGG. *Bilaga 2: Klassificering av statliga myndigheter 2022* (2023)
<https://www.digg.se/download/18.5d519bdf18bdf9fbd001191a/1701168602278/Bilaga%202%20Klassificering%20av%20statliga%20myndigheter%202022.pdf> (2024-04-03)
- DIGG. *Digitalisering för förvaltningsgemensam nytta*. (2023) <https://www.digg.se/analys-och-uppfoljning/publikationer/publikationer/2023-09-06-digitalisering-for-forvaltning-gemensam-nytta> (2024-04-10)
- Ekholm, Anders; Jebari, Karim och Markovic, Drasko. *Förbjuden framtid? Den digitala kommunen* (Institutet för Framtidsstudier 2018)
<https://www.iffs.se/publikationer/ovrigt/forbjuden-framtid/>
- Europeiska unionens officiella tidning. *Europaparlamentets och rådets förordning (EU) 2024/1183* (2024) https://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=OJ:L_202401183#d1e3705-1-1 (2024-05-29)
- Skatteverket. *Folkbokföringsdatabasen*. (u.å.)
<https://skatteverket.se/privat/folkbokforing/attvarafolkbokford/folkbokforingsdatabasen.4.3810a01c150939e893f16fe2.html> (2024-04-09)
- Skatteverket. *Organisationsnummer*. (u.å.)
<https://skatteverket.se/foretag/drivaforetag/startaochregistrera/organisationsnummer.4.361dc8c15312eff6fd235a1.html> (2024-04-09)
- Statskontoret. *Myndigheternas storlek* (u.å.)
<https://www.statskontoret.se/fokusomraden/fakta-om-statsforvaltningen/myndigheternas-storlek/> (2024-04-09)
- Sveriges kommuner och regioner. *Vad kommer det att kosta socialtjänsten att investera i digitala lösningar?* (2024)
<https://skr.se/skr/integrationsocialomsorg/socialomsorg/digitaliseringinomsocialtjansten/verktygochutvecklingsarbeten/kostnaderdigitaliseringsocialtjansten.32340.html> (2024-05-09)
- Transportstyrelsen. *Organisation*. (2024) <https://www.transportstyrelsen.se/sv/om-transportstyrelsen/organisation/> (2024-05-02)
- Universitets- och högskolerådet (UHR). *Reglerade yrken* (2024)
<https://www.uhr.se/bedomning-av-utlandsk-utbildning/arbete-och-studier/arbete-i-Sverige/Reglerade-yrken/> (2024-04-04)
- Universitets- och högskolerådet (UHR). *Beda – nationella betygsdatabasen*. (2021)
<https://www.uhr.se/systemtjanster-for-larosaten/stodsystem-for-larosaten/betygsdatabasen-beda/> (2024-05-02)
- Wikipedia. *Lista över Sveriges kommuner*. (u.å.)
https://sv.wikipedia.org/wiki/Lista_%C3%B6ver_Sveriges_kommuner (2024-05-02)



Bilagor

Bilaga 1: Kartläggning av berörda aktörer

Attributintyg	Typ av information	Informationens källa
Adress	Folkbokföring	Skatteverket
Ålder	Folkbokföring	Skatteverket
Kön	Folkbokföring	Skatteverket
Civil status	Folkbokföring	Skatteverket
Familjesammansättning	Folkbokföring	Skatteverket
Utbildningskvalifikationer, titlar och licenser	Grundskolebehörighet (Intyg) och betyg	Enskilda kommuner
	Gymnasieexamen	
	Eftergymnasial examen (Kandidat, Master och forskarnivå)	Universitet
	Examen från Yrkehögskola	Myndigheten för yrkehögskolan
Yrkeskvalifikationer, titlar och licenser	Auktoriserad tolk och translator	Kammarkollegiet
	Aktuarie	Finansinspektionen
	Bergsguide	Universitets och högskolerådet
	Besprutning av skadedjur och insekter	Folkhälsomyndigheten
	Besprutning av skadedjur och insekter	Arbetsmiljöverket
	Brandskyddskontroll	Myndigheten för samhällsskydd och beredskap
	Elinstallatör	Elsäkerhetsverket
	Fastighetsmäklare och hyresförmedlare	Fastighetsmäklarinspektionen
	Apotekare	Socialstyrelsen
	Arbsterapeut	
	Audionom	
	Barnmorska	
	Biomedicinsk analytiker	



	Dietist	
	Fysioterapeut	
	Hälsa- och sjukvårdskurator	
	Kiropraktor	
	Logoped	
	Läkare och specialtläkare	
	Naprapat	
	Optiker	
	Ortopedingenjör	
	Psykolog	
	Psykoaterapeut	
	Receptarie	
	Röntgensjuksköterska	
	Sjukhusfysiker	
	Sjuksköterska och specialistsjuksköterska	
	Tandhygienist	
	Tandläkare och specialisttandläkare	
	Undersköterska	
	Yrkesverksamma inom den sociala barn- och ungdomsvården	
	Djursjukskötare	
	Djurvårdare utökad nivå	
	Fysioterapeut och tandläkare inom djurens hälsa- och sjukvård (legitimerad enligt patientsäkerhetslagen (2010:659) godkänd för verksamhet inom djurens hälsa- och sjukvård)	Jordbruksverket
	Godkänd hovslagare	
	Veterinär	
	Besprutning av växter, grus, asfalt m.m.	
	Lärare och förskolelärare offentligt	Skolverket
	Patentombud	Patentsombudsämnden
	Sakkunniga inom brandskydd, funktionskontroll, kulturvärden och tillgänglighet	Boverket
	Energiexpert	
	Kontrollansvarig	



	Kontroll av hissar	
	Väktare	Länsstyrelser
	Revisor	Revisorinspektionen
	Yrken inom sjöfart och flyg	Transportstyrelsen
	Taxiförare	
	Trafiklärare	
	Forsrännare	
	Besiktningstekniker	
	Polisen	Polismyndigheten
	Försvaret	Försvarsmakten
Befattningar inom rättsväsendet	Sveriges domstolar	
<i>Befogenheter och mandat att företräda fysisk eller juridisk person</i>		
<i>Offentliga tillstånd och licenser</i>	Tillstånd relaterade till trafik	Transportstyrelsen Trafikverket
	Polisiära tillstånd som demonstrationstillstånd och vapenlicens	Polismyndigheten
	Uppehållstillstånd övriga liknande.	Migrationsverket
	Elektronisk kommunikation	Post- och telestyrelsen
	Immateriell rätt	Patent- och registreringsverket
	Utbildning	Skolinspektionen
	Olika typer av fastighetstillstånd, spridningstillstånd.	Lantmäteriet
	Tillstånd för mäklare och mäklarfirmor	Fastighetsmäklarinspektionen
	Auktorisering av revisorer, registrering av revisionsbolag, tillstånd för att utföra lagstadgad revision inom särskilda områden.	Revisorinspektionen
	Intyg om giftermål, tillstånd och intyg kopplat till organisationers ekonomiska delar.	Skatteverket
	Banktillstånd, försäkringstillstånd, tillstånd för kreditmarknadsbolag, tillstånd för betaltjänstleverantörer m.m.	Finansinspektionen
	Tillstånd för fristående skolor	Skolverket
Tillstånd gällande ansökningar till universitet och högskolor	Universitets och högskolerådet	



	Tillstånd för vissa farliga kemiska produkter, tillstånd om bekämpningsmedel, tillstånd för biocidprodukter, tillstånd för vissa särskilda ämnen.	Kemikalieinspektionen
	Tillstånd gällande bolagsformer och bolagsstrukturer	Bolagsverket
	Tillstånd för exportlicens och importtillstånd	Kommerskollegium
	Tillstånd om icke-statlig verksamhet i yttre rymden	Rymdstyrelsen
	Tillstånd för verksamheter som bedriver vård och omsorg	Inspektionen för vård och omsorg
		Exportkreditnämnden
	Hälso- och sjukvårdstillstånd	Socialstyrelsen
	Press och media	Statens medieråd
	Etikprövningstillstånd för forskning på människor, godkännande för kliniska prövningar av läkemedel, tillstånd för användning av vissa biologiska material, tillstånd för användning av personuppgifter i forskning	Etikprövningsmyndigheten
	Tillstånd för sändning av radio och TV, tillstånd för publicering av databas	Myndigheten för press, radio och tv
	Undersökningstillstånd	Sveriges geologiska undersökning (SGU)
	Tillstånd kopplade till produktion och försäljning av energi	Energimarknadsinspektionen
		E-Hälsomyndigheten
	Bygglov, marklov, serveringstillstånd, miljöstillstånd, V-A tillstånd, försäljningstillstånd	Enskilda kommuner
Länsstyrelsers tillstånd	Respektive länsstyrelse	
För juridiska personer, finans- och företagsdata	Näringslivsregistret	Bolagsverket
	Aktiebolag	
	Bostadsrättsföreningar	
	Ekonomiska föreningar	
	Europeisk ekonomisk intressegruppering – EEIG	
	Europeisk gruppering för territoriellt samarbete – EGTS	
	Europabolag	



	Europakooperativ	
	Kooperativa	
	Hyresrättsföreningar	
	Handelsbolag	
	Kommanditbolag	
	Utländska företags filialer	
	Bankaktiebolag	
	Försäkringsaktiebolag	
	Försäkringsföreningar	
	Sparbanker	
	Medlemsbanker	
	Bankfilial	
	Utländska bankers filialer	
	Ömsesidiga försäkringsbolag	
	Arbetslöshetskassor	Inspektionen för arbetslöshetsförsäkringen
	Allmänna försäkringskassor	
	Hypoteksföreningar	
	Kommunalförbund	
	Offentliga korporationer och anstalter	Statistiska centralbyrån
	Kommuner	
	Regionala statliga myndigheter	
	Regioner	
	Statliga myndigheter	
	Vattenförbund	Respektive länsstyrelse
	Samfällighetsföreningar	Lantmäteriet
	Vägföreningar	
	Registrerat trossamfund	Kammarkollegiet
	Enkla bolag	
	Eric-konsortium	
	Familjestiftelser	
	Ideella föreningar	Skatteverket
	Oskiftade dödsbon	
	Partrederier	
	Övriga stiftelser och fonder	
	Utländska juridiska personer	



Bilaga 2: Urvalskriterier gällande digital mognad

DIGG arbetar med att bistå regeringen med underlag för utvecklingen av digitaliseringen av den offentliga förvaltningen. Det innebär att följa och analysera utvecklingen inom området. En del i detta uppdrag är att undersöka den digitala mognaden inom statliga myndigheter. För att göra detta skickar DIGG ut en årlig enkät till svenska myndigheter som är frivillig att besvara. Frågorna som ställs har att göra med olika aspekter av digital mognad och ligger till grund för fyra olika index, dessa är samverkansindex, teknologiindex, diggindex och mognadsindex. Vilka frågor som utgör respektive index framgår nedan. Värdet för respektive index på myndighetsnivå har tillhandhållits av DIGG. Mätningen från 2023 är fortfarande under bearbetning, alltså är mätningen från 2022 den senaste att tillgå.

För det här uppdraget har enkätundersökningen syftat till att ge underlag för att kunna särskilja på identifierade berörda myndigheters digitala mognad. Digital mognad har framkommit som en avgörande faktor för hur dyrt det kommer att bli att ställa om till eIDAS-förordningens bilaga VI.

Ett problem med detta är att alla index inte mäter faktorer som nödvändigtvis är relevanta för denna undersökning. Därmed har endast diggindexet valts ut för undersökningen. Som underlag för detta val har samtliga frågor kategoriserats utifrån relevans för undersökningen, därefter framkom diggindexet som det bäst lämpade.

Teknologiindex 2022

15. Vilken/ vilka av nedanstående tekniker använder ni idag i er verksamhet?
Automatiserad handläggning.

- Automatiserade beslut.
- Big Data-analys.
- Maskininlärning.
- Dialogrobotar (chatbots).
- Robotic Process Automation (RPA).
- Blockkedjeteknik.
- Annan "ny" teknologi (fritextsvar).

Diggindex 2022

27. På vilket sätt tillgängliggör ni information digitalt? Gör en totalbedömning.
Vi skickar information digitalt till specifika aktörer.

- Vi publicerar information i form av dokument (t ex Word eller pdf) eller som text på vår webbsida.
- Vi publicerar information i form av statiska filer (t ex Excel eller CSV).
- Vi tillgängliggör information genom programmeringsgränssnitt, s k API:er.
- Vi publicerar dynamiska data, dvs data som uppdateras frekvent eller i realtid.
- Vi publicerar metadata om vår information.



- Vi använder öppna, maskinläsbara och vedertagna licenser och/eller rättighetsmärkning.

28. Tillgängliggör ni digital information för vidareutnyttjande?

29. Fråga om hur olika typer av digital information tillgängliggörs för vidareutnyttjande. Vi tillgängliggör...

- ...upprättade register inom
- verksamhetens kärnuppdrag
- ...beslut
- ...diarium
- ...handläggningstider
- ...statistik
- ...ekonomisk information (t ex årsredovisningsdata)
- ...inköpsdata (t ex leverantörsfakturer)
- ...avtal
- ...annan information (fritextsvar)

33. Följer ni upp resultatet av er digitala verksamhetsutveckling? Vi följer upp...
...vår digitala mognad.

- ...digitaliseringsgraden i vår
- kärnverksamhet.
- ...digitaliseringsgraden i vår stödverksamhet.
- ...hur våra digitala lösningar bidrar
- till en sammanhållen verksamhetsarkitektur.
- ...våra digitala lösningars användbarhet/ tillgänglighet.
- ...våra digitala lösningar ur ett rättssäkerhetsperspektiv.
- ...våra målgruppers uppfattning om vår digitala service.

37. På vilket sätt tar ni hänsyn till era målgruppers behov vid utveckling av digitala lösningar?

- Målgrupperna kan finnas både inom och utom offentlig förvaltning, och även internt inom myndigheten.
- Vi samlar in behov, önskemål etc från våra målgrupper (t ex genom enkätundersökningar, fokusgrupper).
- Vi analyserar målgruppernas behov utifrån livshändelser/ företagshändelser (t ex genom att ta fram sk kundresor).
- Vi involverar målgrupperna i vårt utvecklingsarbete (tex för att testa nya lösningar, beskriva specifika behov eller föreslå förbättringar).
- Vi mäter nöjdheten/upplevelsen hos våra målgrupper (t ex genom NKI-mätningar).
- Vi tar hänsyn till målgruppernas behov på annat sätt (fritextsvar).

49. Använder ni Mina meddelanden för utskick till privatpersoner, företag eller intresseorganisationer?



Mognadsindex 2022

5. Hur bedömer ni kompetensen hos myndighetens ledning när det gäller att... Gör en totalbedömning.

- ...bedöma hur den digitala utvecklingen påverkar er verksamhet?
- ...avgöra hur digital teknik kan användas för att utveckla servicen till era målgrupper?
- ...avgöra hur digital teknik kan användas för att utveckla er interna verksamhet?
- ...avgöra hur digital teknik kan säkerställa korrekta beslut?

6. Hur bedömer ni kompetensen hos myndighetens medarbetare när det gäller att... Gör en totalbedömning.

- ...bedöma hur den digitala utvecklingen påverkar er verksamhet?
- ...avgöra hur digital teknik kan användas för att utveckla servicen till era målgrupper?
- ...avgöra hur digital teknik kan användas för att utveckla er interna verksamhet?
- ...avgöra hur digital teknik kan användas för att utveckla riskanalyser och kontroller för att motverka felaktiga beslut/felaktiga utbetalningar?
- ...tillämpa digital teknik för att utveckla er verksamhet?

7. Har er digitala verksamhetsutveckling resulterat i genomgripande förbättringar under det senaste året och i så fall på vilket sätt?

8. Bedriver ni systematiskt arbete...

- ...för omvärlds- och trendanalys?
- ...för att fånga upp och utveckla nya idéer?
- ...för att hantera initiativ och förslag till utveckling från era målgrupper?
- ...för att arbeta med verksamhetsarkitektur?
- ...för att prioritera mellan olika utvecklingsinitiativ?
- ...för att arbeta med itarkitektur?
- ...för att bedöma och hantera risker kopplade till era digitala lösningar?
- ...för att säkerställa att er verksamhetsutveckling fokuserar på förväntad nytta/effekt?
- ...för att realisera nyttor/effekter av genomförda utvecklingsinitiativ?

10. I vilken utsträckning stämmer nedanstående påståenden för er hantering av den information ni använder i verksamheten? Gör en totalbedömning.

- Vi har inventerat och förtecknat vår information.
- Vi har genomfört säkerhetsklassning av vår information.
- Vi har utsett informationsägare för vår information.
- Vår information är kvalitetssäkrad.
- Vår information är bevarad på ett säkert sätt.
- Vår information finns tillgänglig i ett strukturerat format.
- Vår information är beskriven i form av metadata.
- Vi arbetar systematiskt med informationsarkitektur.

19. Frågar ni enskilda om uppgifter som redan finns hos andra offentliga organisationer?

21. På vilket sätt hämtar ni uppgifter om enskilda från andra offentliga organisationer?



- Genom direktåtkomst till aktuella uppgifter via en tjänst (t ex bastjänst), delade data (t ex API) eller delade system.
 - Genom att återkommande hämta in/ta emot statiska uppgifter från andra (t ex via filöverföring eller direktinmatning).
 - På annat sätt (fritextsvar).
22. Har er myndighet antagit principen "öppet som standard", dvs att verksamheten ska sträva efter att göra att information öppen och digitalt tillgänglig för användning av externa intressenter? Enbart den information som är skyddsvärd ska särbehandlas.
25. Har er myndighet tekniska möjligheter att digitalt avidentifiera uppgifter som omfattar skyddsvärd information?
27. På vilket sätt tillgängliggör ni information digitalt? Gör en totalbedömning.
- Vi skickar information digitalt till specifika aktörer.
 - Vi publicerar information i form av dokument (t ex Word eller pdf) eller som text på vår webbsida.
 - Vi publicerar information i form av statiska filer (t ex Excel eller CSV).
 - Vi tillgängliggör information genom programmeringsgränssnitt, s k API:er.
 - Vi publicerar dynamiska data, dvs data som uppdateras frekvent eller i realtid.
 - Vi publicerar metadata om vår information.
 - Vi använder öppna, maskinläsbara och vedertagna licenser och/eller rättighetsmärknings.
28. Tillgängliggör ni digital information för vidareutnyttjande?
29. Fråga om hur olika typer av digital information tillgängliggörs för vidareutnyttjande. Vi tillgängliggör...
- ...upprättade register inom verksamhetens kärnuppdrag
 - ...beslut
 - ...diarium
 - ...handläggningstider
 - ...statistik
 - ...ekonomisk information (t ex årsredovisningsdata)
 - ...inköpsdata (t ex leverantörsfakturor)
 - ...avtal
 - ...annan information (fritextsvar)
31. På vilka sätt skapas incitament för digital verksamhetsutveckling hos er? Gör en totalbedömning.
- Myndighetens instruktion (uppdrag) ger tydliga incitament till digital verksamhetsutveckling.
 - Vårt regleringsbrev betonar tydligt vikten av digital verksamhetsutveckling.
 - Vi har specifika regeringsuppdrag som avser digital verksamhetsutveckling.
 - Beslutade EU förordningar initierar insatser inom vår digitala verksamhetsutveckling.
 - Ekonomiska incitament driver vår digitala verksamhetsutveckling.



- Incitament kopplade till korrekta beslut/korrekta utbetalningar driver vår digitala verksamhetsutveckling.
 - Resultaten från vårt uppföljningsarbete/våra nyttoanalyser initierar insatser inom vår digitala verksamhetsutveckling.
 - Vi har interna mål som driver den digitala verksamhetsutvecklingen.
 - Utveckling av digitala lösningar ingår som en naturlig del i våra verksamhetsutvecklingsinitiativ.
33. Följer ni upp resultatet av er digitala verksamhetsutveckling? Vi följer upp...
- ...vår digitala mognad.
 - ...digitaliseringsgraden i vår kärnverksamhet.
 - ...digitaliseringsgraden i vår stödverksamhet.
 - ...hur våra digitala lösningar bidrar till en sammanhållen verksamhetsarkitektur.
 - ...våra digitala lösningars användbarhet/ tillgänglighet.
 - ...våra digitala lösningar ur ett rättssäkerhetsperspektiv.
 - ...våra målgruppers uppfattning om vår digitala service.
36. I vilken utsträckning stämmer nedanstående påståenden för er utveckling av digitala lösningar?
- Vi genomför egen utveckling av digitala lösningar.
 - Vi utkontrakterar vår utveckling av digitala lösningar till externa leverantörer.
 - Vi köper in färdiga tjänster/ programvaror när vi har behov av digitala lösningar.
 - Vi lämnar "fritt" till andra att genomföra utvecklingsarbetet genom att dela med oss av data.
 - Annat (fritextsvar).
39. I vilken utsträckning återanvänder ni...
- ...egna befintliga lösningar att bygga vidare på istället för att utveckla nytt från grunden?
 - ...underlag, arkitekturmönster, lösningar (t ex förvaltningsgemensamma tjänster) etc som utarbetats av andra offentliga eller privata aktörer?
41. Underlättar ni för andra offentliga aktörer att återanvända ert utvecklingsarbete genom att...
- ...efter förfrågan dela med er av underlag, arkitekturmönster, lösningar etc?
 - ...öppet publicera underlag, arkitekturmönster, lösningar etc?
 - ...skapa kataloger över de digitala tjänster, samverkans-lösningar etc som ni utvecklar?
 - ...erbjuda externa gränssnitt till era digitala tjänster (t ex genom API:er)?
 - ...erbjuda andra aktörer att genom samverkan eller samarbete delta vid vidareutveckling av era lösningar?
42. Hur ser er samverkan med andra ut kopplat till utveckling av digitala lösningar?
- ...genom analys av livshändelseperspektiv.
 - ...inom teknisk utveckling av digitala tjänster/lösningar.
 - ...genom arbete med standarder, specifikationer etc
 - ...genom arbete kring juridiska aspekter vid utveckling av digitala lösningar
 - ...genom gemensamma riskanalyser



- ...genom att tillhandahålla gemensamma digitala kontaktpunkter tillsammans med andra (t ex för vägledning, information eller tillgång till digitala tjänster)
 - ...genom att erbjuda gemensamma integrerade digitala tjänster tillsammans med andra
 - ...inom annat område (fritextsvar)
47. Är det möjligt för användare att följa sitt ärende i era digitala tjänster?'
48. Använder era digitala tjänster data eller information som tagits fram eller förvaltas av andra offentliga eller privata aktörer?
49. Använder ni Mina meddelanden för utskick till privatpersoner, företag eller intresseorganisationer?

Samverkansindex 2022

19. Frågar ni enskilda om uppgifter som redan finns hos andra offentliga organisationer?
21. På vilket sätt hämtar ni uppgifter om enskilda från andra offentliga organisationer?
- Genom direktåtkomst till aktuella uppgifter via en tjänst (t ex bastjänst), delade data (t ex API) eller delade system.
 - Genom att återkommande hämta in/ta emot statiska uppgifter från andra (t ex via filöverföring eller direktinmatning).
 - På annat sätt (fritextsvar).
22. Har er myndighet antagit principen "öppet som standard", dvs att verksamheten ska sträva efter att göra att information öppen och digitalt tillgänglig för användning av externa intressenter? Enbart den information som är skyddsvärd ska särbehandlas.
28. Tillgängliggör ni digital information för vidareutnyttjande?
39. I vilken utsträckning återanvänder ni...
- ...egna befintliga lösningar att bygga vidare på istället för att utveckla nytt från grunden?
- ...underlag, arkitekturmönster, lösningar (t ex förvaltningsgemensamma tjänster) etc som utarbetats av andra offentliga eller privata aktörer?
41. Underlättar ni för andra offentliga aktörer att återanvända ert utvecklingsarbete genom att...
- ...efter förfrågan dela med er av underlag, arkitekturmönster, lösningar etc?
 - ...öppet publicera underlag, arkitekturmönster, lösningar etc?
 - ...skapa kataloger över de digitala tjänster, samverkans-lösningar etc som ni utvecklar?
 - ...erbjuda externa gränssnitt till era digitala tjänster (t ex genom API:er)?
 - ...erbjuda andra aktörer att genom samverkan eller samarbete delta vid vidareutveckling av era lösningar?"
42. Hur ser er samverkan med andra ut kopplat till utveckling av digitala lösningar?
48. Använder era digitala tjänster data eller information som tagits fram eller förvaltas av andra offentliga eller privata aktörer?

Statens offentliga utredningar 2024

Kronologisk förteckning

1. Ett starkare skydd för offentliganställda mot våld, hot och trakasserier. Ju.
2. Ett samordnat vaccinationsarbete – för effektivare hantering av kommande vacciner. Del 1 och 2. S.
3. Ett starkt juridiskt liv för framtida generationer. Nationell strategi för att stärka juridiskt liv i Sverige 2025–2034. Ku.
4. Inskränkningarna i upphovsrätten. Ju.
5. Förbättrad ordning och säkerhet vid förvar. Ju.
6. Steg mot stärkt kapacitet. Fi.
7. Ett säkrare och mer tillgängligt fastighetsregister. Ju.
8. Livsmedelsberedskap för en ny tid. LI.
9. Utvecklat samarbete för verksamhetsförlagd utbildning – långsiktiga åtgärder för sjuksköterskeprogrammen. U.
10. Preskription av avlägsnandebeslut och vissa frågor om återreseförbud. Ju.
11. Rätt frågor på regeringens bord – en ändamålsenlig regeringsprövning på miljöområdet. KN.
12. Mål och mening med integration. A.
13. En effektivare kontaktförbudslagstiftning – ett utökad skydd för utsatta personer. Ju.
14. Arbetslivskriminalitet – myndighets-samverkan, en gemensam tipsfunktion, lärdomar från Belgien och gränsöverskridande arbete. A.
15. Nya regler för arbetskraftsinvandring m.m. Ju.
16. Växla yrke som vuxen – en reformerad vuxenutbildning och en ny yrkesskola för vuxna. U.
17. Skolor mot brott. U.
18. Nya regler om cybersäkerhet. Fö.
19. En ny beredskapssektor – för ökad försörjningsberedskap. KN.
20. Maskinellt värde för vissa industribyggnader – ett undantag från fastighets-skatt. Fi.
21. Ett inkluderande jämställdhetspolitiskt delmål mot våld. A.
22. En ny organisation för förvaltning av EU-medel. Fi.
23. En trygg uppväxt utan nikotin, alkohol och lustgas. S.
24. Ett effektivt straffrättsligt skydd för statliga stöd till företag. Fi.
25. En mer effektiv tillsyn över socialtjänsten. S.
26. En utvärdering av förändringar i sjukförsäkringens regelverk under 2021 och 2022. S.
27. Kamerabevakning i offentlig verksamhet – lättnader och utökade möjligheter. Ju.
28. Offentlighetsprincipen eller insyns-lag. Allmänhetens insyn i enskilda aktörer inom skolväsendet. U.
29. Goda möjligheter till ökat välbefinnande. Fi.
30. En statlig ordning med brottsförebyggande åtgärder för barn och unga. S.
31. En ändamålsenlig vapenlagstiftning. Del 1 och 2. Ju.
32. Åtgärder mot mervärdesskattebedrägerier. Fi.
33. Delad hälsodata – dubbel nytta. Regler för ökad interoperabilitet i hälso- och sjukvården. S.
34. Ansvar och oberoende – public service i oroliga tider. Ku.
35. En framtid för alm och ask – förädling, forskning och finansiering. LI.

36. Förenkla och förbättra! Fi.
37. Förbättrade ränteavdragsregler för företag. Fi.
38. Digitala fastighetsköp & Förförsköprätt vid fastighetstransaktioner. LI.
39. Skärpta regler om ungdomsövervakning och straffreduktion för unga. Ju.
40. Genomförande av lönetransparensdirektivet. A.
41. Styrkraft för lyckad integration. A.
42. Bildning, utbildning och delaktighet – folkbildningspolitik i en ny tid. U.
43. Staten och kommunsektorn – samverkan, självstyrelse, styrning. Fi.
44. Stärkt kontroll av fusk i livsmedelskedjan. LI.
45. Kompletterande bestämmelser till EU:s reviderade förordning om elektronisk identifiering. Fi.

Statens offentliga utredningar 2024

Systematisk förteckning

Arbetsmarknadsdepartementet

- Mål och mening med integration. [12]
- Arbetslivskriminalitet – myndighets-samverkan, en gemensam tipsfunktion, lärdomar från Belgien och gränsöver-skridande arbete. [14]
- Ett inkluderande jämställdhetspolitiskt delmål mot våld. [21]
- Genomförande av lönetransparensdirektivet. [40]
- Styrkraft för lyckad integration. [41]

Finansdepartementet

- Steg mot stärkt kapacitet. [6]
- Maskinellt värde för vissa industribyggnader – ett undantag från fastighetsskatt. [20]
- En ny organisation för förvaltning av EU-medel [22]
- Ett effektivt straffrättsligt skydd för statliga stöd till företag. [24]
- Goda möjligheter till ökat välbefinnande. [29]
- Åtgärder mot mervärdesskattebedrägerier. [32]
- Förenkla och förbättra! [36]
- Förbättrade ränteavdragsregler för företag. [37]
- Staten och kommunsektorn – samverkan, självstyrelse, styrning. [43]
- Kompletterande bestämmelser till EU:s reviderade förordning om elektronisk identifiering. [45]

Försvarsdepartementet

- Nya regler om cybersäkerhet. [18]

Justitiedepartementet

- Ett starkare skydd för offentliganställda mot våld, hot och trakasserier. [1]
- Inskränkningarna i upphovsrätten. [4]

- Förbättrad ordning och säkerhet vid förvar. [5]
- Ett säkrare och mer tillgängligt fastighetsregister. [7]
- Preskription av avlägsnandebeslut och vissa frågor om återreseförbud. [10]
- En effektivare kontaktförbudslagstiftning – ett utökat skydd för utsatta personer. [13]
- Nya regler för arbetskraftsinvandring m.m. [15]
- Kamerabevakning i offentlig verksamhet – lättnader och utökade möjligheter. [27]
- En ändamålsenlig vapenlagstiftning. Del 1 och 2. [31]
- Skärpta regler om ungdomsövervakning och straffreduktion för unga. [39]

Klimat- och näringslivsdepartementet

- Rätt frågor på regeringens bord – en ändamålsenlig regeringsprövning på miljöområdet. [11]
- En ny beredskapssektor – för ökad försörjningsberedskap. [19]

Kulturdepartementet

- Ett starkt judiskt liv för framtida generationer. Nationell strategi för att stärka judiskt liv i Sverige 2025–2034. [3]
- Ansvar och oberoende – public service i oroliga tider. [34]

Landsbygds- och infrastrukturdepartementet

- Livsmedelsberedskap för en ny tid. [8]
- En framtid för alm och ask – förädling, forskning och finansiering. [35]
- Digitala fastighetsköp & Förköpsrätt vid fastighetstransaktioner. [38]

Stärkt kontroll av fusk i livsmedelskedjan.
[44].

Socialdepartementet

Ett samordnat vaccinationsarbete – för effektivare hantering av kommande vacciner. Del 1 och 2. [2]

En trygg uppväxt utan nikotin, alkohol och lustgas. [23]

En mer effektiv tillsyn över socialtjänsten. [25]

En utvärdering av förändringar i sjukförsäkringens regelverk under 2021 och 2022. [26]

En statlig ordning med brottsförebyggande åtgärder för barn och unga. [30]

Delad hälsodata – dubbel nytta. Regler för ökad interoperabilitet i hälso- och sjukvården. [33]

Utbildningsdepartementet

Utvecklat samarbete för verksamhetsförlagd utbildning – långsiktiga åtgärder för sjuksköterskeprogrammen. [9]

Växla yrke som vuxen – en reformerad vuxenutbildning och en ny yrkesskola för vuxna. [16]

Skolor mot brott. [17]

Offentlighetsprincipen eller insynslag. Allmänhetens insyn i enskilda aktörer inom skolväsendet. [28]

Bildning, utbildning och delaktighet – folkbildningspolitik i en ny tid. [42]