Lena Persson

Från: Maria Solberg <maria.solberg@regeringskansliet.se> för I ESD remisser <i.esd.remisser@regeringskansliet.se>
Skickat: den 21 november 2022 10:57
Till: Maria Solberg
Kopia: 'betankande@elanders.com'
Ämne: Remiss av Europeiska kommissionens förslag till förordning om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordning (EU) 2019/1020 - Svar senast 21/2 2023
Bifogade filer: Remissmissiv CRA.pdf; Cyberresiliensakten_se.pdf; Bilagor till Cyberresiliensakten_se.pdf

Uppföljningsflagga: Följ upp
Flagga: Har meddelandeflagga

Kategorier: Lena

Remiss av Europeiska kommissionens förslag till förordning om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordning (EU) 2019/1020

Remissinstanser

1 AB Electrolux
2 AB LM Ericsson
3 ABB Electrification Sweden AB
4 Affärsverket svenska kraftnät
5 AI Sweden
6 Assa Abloy AB
7 Atlas Copco AB
8 Business Sweden
9 Chalmers tekniska högskola
10 Civic Tech Sweden
11 Combient AB
12 Combitech AB
13 Dataföreningen
14 Ekonomistyrningsverket
15 Elsäkerhetsverket
16 Energiföretagen
17 Energimyndigheten
18 Företagarna
19 Försvarets materielverk
20 Försvarets radioanstalt
21 Försvarsmakten

22 Innovationsföretagen
23 Inspektionen för strategiska produkter
24 Integritetsskyddsmyndigheten
25 Internetstiftelsen
26 IoT Sverige
27 Kommerskollegium
28 Konsumentombudsmannen
29 Konsumentverket
30 Kungliga Ingenjörsvetenskapsakademien
31 Kungliga tekniska högskolan
32 Lindholmen Science Park AB
33 Myndigheten för digital förvaltning
34 Myndigheten för samhällsskydd och beredskap
35 Näringslivets Regelnämnd
36 Patent- och registreringsverket
37 Polismyndigheten
38 Post- och telestyrelsen
39 Power Circle AB
40 Regelrådet
41 Research Institutes of Sweden AB RISE
42 SAAB AB
43 Svensk handel
44 Svenska föreningen för IT och juridik
45 Svenska informations- och telekommunikationsstandardiseringen
46 Svenska institutet för standarder
47 Svenskt näringsliv
48 Swedac
49 Swedsoft
50 Säkerhets- och försvarsföretagen
51 Säkerhetspolisen
52 Tech alliansen
53 TechSverige
54 Teknikföretagen
55 The Wallenberg AI, Autonomous Systems and Software Program
56 Tillväxtverket
57 Totalförsvarets forskningsinstitut
58 Trafikverket
59 Tullverket
60 Verket för innovationssystem
61 Vetenskapsrådet

Remissvaren ska ha kommit in till Finansdepartementet **senast den 21 februari 2023**. Svaren bör lämnas per e-post till i.remissvar@regeringskansliet.se och med kopia till i.esd.remisser@regeringskansliet.se. Ange diarienummer I2022/01758 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 förslaget. **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.

Önskas ett fysiskt exemplar av remissen, vänligen kontakta Sanna Cecilgård, e-post: sanna.cecilgard@regeringskansliet.se, telefon: 08-405 89 60. 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.

Staffan Lindmark
Departementsråd

Regeringskansliet

Remiss

2022-11-21
I2022/01758

Infrastrukturdepartementet
Enheten för samhällets digitalisering

Europeiska kommissionens förslag till förordning om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordning (EU) 2019/1020

Remissinstanser

1 AB Electrolux
2 AB LM Ericsson
3 ABB Electrification Sweden AB
4 Affärsverket svenska kraftnät
5 AI Sweden
6 Assa Abloy AB
7 Atlas Copco AB
8 Business Sweden
9 Chalmers tekniska högskola
10 Civic Tech Sweden
11 Combient AB
12 Combitech AB
13 Dataföreningen
14 Ekonomistyrningsverket
15 Elsäkerhetsverket
16 Energiföretagen
17 Energimyndigheten
18 Företagarna
19 Försvarets materielverk

Telefonväxel: 08-405 10 00
Fax: 08-24 46 31
Webb: www.regeringen.se

Postadress: 103 33 Stockholm
Besöksadress: Malmtorgsgatan 3
E-post: i.registrator@regeringskansliet.se

20 Försvarets radioanstalt
21 Försvarsmakten
22 Innovationsföretagen
23 Inspektionen för strategiska produkter
24 Integritetsskyddsmyndigheten
25 Internetstiftelsen
26 IoT Sverige
27 Kommerskollegium
28 Konsumentombudsmannen
29 Konsumentverket
30 Kungliga Ingenjörsvetenskapsakademien
31 Kungliga tekniska högskolan
32 Lindholmen Science Park AB
33 Myndigheten för digital förvaltning
34 Myndigheten för samhällsskydd och beredskap
35 Näringslivets Regelnämnd
36 Patent- och registreringsverket
37 Polismyndigheten
38 Post- och telestyrelsen
39 Power Circle AB
40 Regelrådet
41 Research Institutes of Sweden AB RISE
42 SAAB AB
43 Svensk handel
44 Svenska föreningen för IT och juridik
45 Svenska informations- och telekommunikationsstandardiseringen
46 Svenska institutet för standarder
47 Svenskt näringsliv
48 Swedac
49 Swedsoft
50 Säkerhets- och försvarsföretagen
51 Säkerhetspolisen

52 Tech alliansen

53 TechSverige

54 Teknikföretagen

55 The Wallenberg AI, Autonomous Systems and Software Program

56 Tillväxtverket

57 Totalförsvarets forskningsinstitut

58 Trafikverket

59 Tullverket

60 Verket för innovationssystem

61 Vetenskapsrådet

Remissvaren ska ha kommit in till Finansdepartementet **senast den 21 februari 2023**. Svaren bör lämnas per e-post till i.remissvar@regeringskansliet.se och med kopia till i.esd.remisser@regeringskansliet.se. Ange diarienummer I2022/01758 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 förslaget. **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.

Önskas ett fysiskt exemplar av remissen, vänligen kontakta Sanna Cecilgård, e-post: sanna.cecilgard@regeringskansliet.se, telefon: 08-405 89 60.
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.

Staffan Lindmark
Departementsråd

EUROPEISKA
KOMMISSIONEN

Bryssel den 15.9.2022
COM(2022) 454 final

ANNEXES 1 to 6

BILAGOR

till

FÖRSLAG TILL EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordning (EU) 2019/1020

{SEC(2022) 321 final} - {SWD(2022) 282 final} - {SWD(2022) 283 final}

BILAGA I

VÄSENTLIGA CYBERSÄKERHETSKRAV

1. SÄKERHETSKRAV AVSEENDE EGENSKAPER HOS PRODUKTER MED DIGITALA ELEMENT

(1) Produkter med digitala element ska utformas, utvecklas och produceras på ett sådant sätt att de säkerställer en lämplig cybersäkerhetsnivå baserat på riskerna.

(2) Produkter med digitala element ska levereras utan några kända sårbarheter som kan utnyttjas.

(3) På grundval av den riskbedömning som avses i artikel 10.2, och i tillämpliga fall, ska produkter med digitala element

(a) levereras med en säker standardkonfiguration, inbegripet möjlighet att återställa produkten till dess ursprungliga skick,

(b) säkerställa skydd mot obehörig åtkomst genom lämpliga kontrollmekanismer, inbegripet men inte begränsat till system för autentisering, identitet eller åtkomsthantering,

(c) skydda konfidentialiteten för lagrade, överförda eller på annat sätt behandlade uppgifter, personuppgifter eller andra uppgifter, t.ex. genom kryptering av relevanta data i vila eller i transit med hjälp av de senaste metoderna,

(d) skydda integriteten hos lagrade, överförda eller på annat sätt behandlade uppgifter, personuppgifter eller andra uppgifter, kommandon, program och konfigurationer mot manipulation eller ändringar som inte godkänts av användaren, samt rapporter om datadistorsion,

(e) endast behandla personuppgifter eller andra uppgifter som är adekvata, relevanta och begränsade till vad som är nödvändigt i förhållande till produktens avsedda användning (”minimering av data”),

(f) skydda tillgången till väsentliga funktioner, inbegripet resiliens mot och begränsning av överbelastningsattacker,

(g) minimera sina egna negativa effekter på tillgången till tjänster som tillhandahålls av andra enheter eller nätverk,

(h) utformas, utvecklas och produceras för att begränsa attackytor, inbegripet externa gränssnitt,

(i) utformas, utvecklas och produceras för att minska effekterna av en incident med hjälp av lämpliga mekanismer och tekniker för att begränsa utnyttjandet,

(j) tillhandahålla säkerhetsrelaterad information genom att registrera och/eller övervaka relevant intern verksamhet, inbegripet tillgång till eller ändring av data, tjänster eller funktioner,

(k) säkerställa att sårbarheter kan åtgärdas genom säkerhetsuppdateringar, inbegripet, i tillämpliga fall, genom automatiska uppdateringar och meddelande till användarna om tillgängliga uppdateringar.

2. KRAV PÅ SÅRBARHETSHANTERING

Tillverkare av produkter med digitala element ska

(1) identifiera och dokumentera sårbarheter och komponenter i produkten, bland annat genom att upprätta en programvaruförteckning för material i ett allmänt använt och maskinläsbart format som åtminstone täcker produktens viktigaste (top-level) beroenden,

(2) när det gäller riskerna för produkter med digitala element, utan dröjsmål åtgärda och avhjälpa sårbarheter, bland annat genom att tillhandahålla säkerhetsuppdateringar,

(3) tillämpa effektiva och regelbundna provningar och granskningar av säkerheten hos produkten med digitala element,

(4) när en uppdatering av säkerheten har gjorts tillgänglig, offentligt redovisa information om åtgärdade sårbarheter, inbegripet en beskrivning av sårbarheterna, information som gör det möjligt för användarna att identifiera den produkt med digitala element som påverkas, sårbarheternas konsekvenser, deras allvarlighetsgrad och information som underlättar för användarna att avhjälpa sårbarheterna,

(5) införa och verkställa en policy för samordnad redovisning av sårbarheter,

(6) vidta åtgärder för att underlätta utbyte av information om potentiella sårbarheter i sin produkt med digitala element och i tredjepartskomponenter som ingår i produkten, bland annat genom att tillhandahålla en kontaktadress för rapportering av de sårbarheter som upptäckts i produkten med digitala element,

(7) tillhandahålla mekanismer för säker distribution av uppdateringar av produkter med digitala element för att säkerställa att exploaterbara sårbarheter åtgärdas eller begränsas i tid,

(8) säkerställa att, i de fall då programfixar eller uppdateringar finns tillgängliga för att hantera identifierade säkerhetsproblem, de sprids utan dröjsmål och kostnadsfritt, åtföljda av rådgivande meddelanden som ger användarna relevant information, inbegripet om eventuella åtgärder som ska vidtas.

BILAGA II

INFORMATION OCH INSTRUKTIONER TILL ANVÄNDAREN

Produkten med digitala element ska åtminstone åtföljas av

1. tillverkarens namn, registrerade firmanamn eller registrerade varumärke samt den postadress och e-postadress där tillverkaren kan kontaktas, på produkten eller, om detta inte är möjligt, på förpackningen eller i ett medföljande dokument,
2. den kontaktpunkt där information om produktens sårbarheter i fråga om cybersäkerhet kan rapporteras och tas emot,
3. korrekt identifiering av typ-, parti-, versions- eller serienummer eller annan uppgift som gör det möjligt att identifiera produkten, och motsvarande bruksanvisning och användarinformation,
4. den avsedda användningen, inbegripet den säkerhetsmiljö som tillhandahålls av tillverkaren, samt produktens väsentliga funktioner och information om säkerhetsegenskaperna,
5. varje känd eller förutsebar omständighet, som har samband med användningen av produkten med digitala element i enlighet med dess avsedda ändamål eller under förhållanden där det kan förekomma rimligen förutsebar felaktig användning, som kan leda till betydande cybersäkerhetsrisker,
6. om och, i tillämpliga fall, var programvaruförteckningen finns tillgänglig,
7. i tillämpliga fall, den internetadress där EU-försäkran om överensstämmelse finns tillgänglig,
8. den typ av tekniskt säkerhetsstöd som erbjuds av tillverkaren och hur länge det kommer att tillhandahållas, åtminstone fram till dess att användarna kan förvänta sig att få säkerhetsuppdateringar,
9. detaljerade instruktioner eller en internetadress som hänvisar till sådana detaljerade instruktioner och information om
   (a) nödvändiga åtgärder under den inledande idrifttagningen och under hela produktens livslängd för att säkerställa en säker användning,
   (b) hur ändringar av produkten kan påverka datasäkerheten,
   (c) hur säkerhetsrelevanta uppdateringar kan installeras,
   (d) säker avveckling av produkten, inklusive information om hur användardata kan avlägsnas på ett säkert sätt.

BILAGA III

KRITISKA PRODUKTER MED DIGITALA ELEMENT

Klass I

1. Programvara för identitetshanteringssystem och programvara för hantering av privilegierad åtkomst.
2. Fristående och inbyggda webbläsare.
3. Lösenordshanterare.
4. Programvara som söker efter och avlägsnar skadlig programvara eller sätter den i karantän.
5. Produkter med digitala element som fungerar som virtuella privata nätverk (VPN).
6. System för nätverksförvaltning.
7. Verktyg för hantering av nätverkskonfigurationer.
8. System för övervakning av nättrafik.
9. Förvaltning av nätverksresurser
10. System för säkerhetsinformation och händelsehantering (SIEM).
11. Hantering av uppdateringar/programfixar, inklusive starthanterare.
12. System för hantering av tillämpningskonfigurationer.
13. Programvara för fjärråtkomst/fjärrdelning.
14. Programvara för hantering av mobila enheter.
15. Fysiska nätverksgränssnitt.
16. Operativsystem som inte omfattas av klass II.
17. Brandväggar, intrångsdetektions- och/eller intrångsskyddssystem som inte omfattas av klass II.
18. Routrar, modem avsedda för anslutning till internet och dataväxlar som inte omfattas av klass II.
19. Mikroprocessorer som inte omfattas av klass II.
20. Mikrokontroller.
21. Applikationsspecifika integrerade kretsar (ASIC) och fältprogrammerbara grindmatriser (FPGA) avsedda att användas av väsentliga entiteter av den typ som avses i [bilaga I till direktiv XXX/XXXX (NIS2)].
22. Industriella automatiserings- och kontrollsystem (IACS) som inte omfattas av klass II, t.ex. programmerbara styrsystem (PLC), distribuerade kontrollsystem (DCS), datoriserade numeriska styrenheter för verktygsmaskiner (CNC) och system för övervakning och datainsamling (SCADA).
23. Sakernas internet för industrin som inte omfattas av klass II.

Klass II

1. Operativsystem för servrar, stationära datorer och mobila enheter.
2. Hypervisorer och system för körning av programbehållare som stöder virtualiserad exekvering av operativsystem och liknande miljöer.
3. Infrastruktur för kryptering med öppen nyckel (PKI) och utfärdare av digitala certifikat.
4. Brandväggar, intrångsdetektions- och/eller intrångsskyddssystem avsedda för industriellt bruk.
5. Mikroprocessorer för allmänna ändamål.
6. Mikroprocessorer avsedda för integrering i programmerbara styrenheter och säkra element.
7. Routrar, modem avsedda för anslutning till internet och dataväxlar avsedda för industriellt bruk.
8. Säkra element.
9. Säkerhetsmoduler för hårdvara (HSM).
10. Säkra kryptoprocessorer.
11. Smartkort, smartkortläsare och informationsbärare.
12. Industriella automatiserings- och kontrollsystem (IACS) avsedda att användas av väsentliga entiteter av den typ som avses i [bilaga I till direktiv XXX/XXXX (NIS2)], såsom programmerbara styrsystem (PLC), distribuerade kontrollsystem (DCS), datoriserade numeriska styrenheter för verktygsmaskiner (CNC) och system för övervakning och datainsamling (SCADA).
13. Anordningar för sakernas internet för industrin avsedda att användas av väsentliga entiteter av den typ som avses i [bilaga I till direktiv XXX/XXXX (NIS2)].
14. Komponenter för robotavkänning och robotmanövrering samt robotstyrenheter.
15. Smarta mätare.

BILAGA IV

EU-FÖRSÄKRAN OM ÖVERENSSTÄMMELSE

Den EU-försäkran om överensstämmelse som avses i artikel 20 ska innehålla samtliga uppgifter som anges nedan:

1. Namn och typ samt eventuell ytterligare information som möjliggör unik identifiering av produkten med digitala element.
2. Namn på och adress till tillverkaren eller dennes representant.
3. En förklaring om att EU-försäkran om överensstämmelse utfärdas på leverantörens eget ansvar.
4. Föremål för försäkran (identifiering av produkten så att den kan spåras; vid behov kan ett fotografi bifogas).
5. En förklaring om att det föremål för försäkran som beskrivs ovan överensstämmer med den relevanta harmoniserade unionslagstiftningen.
6. Hänvisningar till relevanta harmoniserade standarder som använts eller andra gemensamma specifikationer eller system för cybersäkerhetscertifiering enligt vilka överensstämmelsen försäkras.
7. I tillämpliga fall, det anmälda organets namn och nummer, en beskrivning av det använda förfarandet för bedömning av överensstämmelse och uppgifter om det utfärdade intyget.
8. Ytterligare information:

Undertecknad för: ……

(ort och datum):

(namn, befattning) (namnteckning):

BILAGA V

DEN TEKNISKA DOKUMENTATIONENS INNEHÅLL

Den tekniska dokumentation som avses i artikel 23 ska åtminstone innehålla följande information, beroende på vad som är tillämpligt för den relevanta produkten med digitala element:

1. En allmän beskrivning av produkten med digitala element, inbegripet
   (a) dess avsedda ändamål,
   (b) versioner av programvara som påverkar överensstämmelsen med de väsentliga kraven,
   (c) om produkten med digitala element är en hårdvaruprodukt, fotografier eller illustrationer som visar yttre egenskaper, märkning och inre layout,
   (d) användarinformation och bruksanvisning enligt bilaga II.
2. En beskrivning av produktens utformning, utveckling och produktion samt processer för sårbarhetshantering, inbegripet
   (a) fullständig information om utformning och utveckling av produkten med digitala element, i tillämpliga fall inbegripet ritningar och scheman och/eller en beskrivning av systemarkitekturen som förklarar hur programvarukomponenter bygger på eller matas in i varandra och integreras i den övergripande behandlingen,
   (b) fullständig information om och specifikationer av de processer för sårbarhetshantering som tillverkaren infört, inbegripet programvaruförteckningen, den samordnade policyn för offentliggörande av sårbarheter, bevis på tillhandahållandet av en kontaktadress för rapportering av sårbarheter och en beskrivning av de tekniska lösningar som valts för säker distribution av uppdateringar,
   (c) fullständig information om och specifikationer av produktions- och övervakningsprocesser för produkten med digitala element och validering av dessa processer.
3. En bedömning av de cybersäkerhetsrisker mot vilka produkten med digitala element utformas, utvecklas, produceras, levereras och underhålls i enlighet med artikel 10 i denna förordning.
4. En förteckning över de harmoniserade standarder som helt eller delvis har följts och till vilka hänvisningar har offentliggjorts i *Europeiska unionens officiella tidning*, gemensamma specifikationer enligt artikel 19 i denna förordning eller system för cybersäkerhetscertifiering enligt förordning (EU) 2019/881 i enlighet med artikel 18.3, och, om dessa harmoniserade standarder, gemensamma specifikationer eller system för cybersäkerhetscertifiering inte har tillämpats, beskrivningar av de lösningar som valts för att uppfylla de väsentliga kraven i avsnitten 1 och 2 i bilaga I, inbegripet en förteckning över andra relevanta tekniska specifikationer som tillämpats. När det gäller delvis tillämpade harmoniserade standarder, gemensamma specifikationer eller system för cybersäkerhetscertifiering ska det i den tekniska dokumentationen specificeras vilka delar som har tillämpats.

5. Rapporter om de provningar som utförts för att kontrollera att produkten och processerna för sårbarhetshantering överensstämmer med de tillämpliga väsentliga kraven i avsnitten 1 och 2 i bilaga I.

6. Kopia av EU-försäkran om överensstämmelse.

7. I tillämpliga fall, programvaruförteckningen enligt definitionen i artikel 3.36, efter en motiverad begäran från en marknadskontrollmyndighet, förutsatt att det är nödvändigt för att denna myndighet ska kunna kontrollera överensstämmelsen med de väsentliga kraven i bilaga I.

BILAGA VI

FÖRFARANDEN FÖR BEDÖMNING AV ÖVERENSSTÄMMELSE

Förfarande för bedömning av överensstämmelse som grundar sig på intern kontroll (baserat på modul A)

1. Intern kontroll är det förfarande för bedömning av överensstämmelse genom vilket tillverkaren fullgör skyldigheterna i punkterna 2, 3 och 4 samt säkerställer och försäkrar på eget ansvar att produkter med digitala element uppfyller alla de väsentliga kraven i avsnitt 1 i bilaga I och att tillverkaren uppfyller de väsentliga kraven i avsnitt 2 i bilaga I.

2. Tillverkaren ska upprätta den tekniska dokumentation som beskrivs i bilaga V.

3. Utformning, utveckling, produktion och sårbarhetshantering av produkter med digitala element

   Tillverkaren ska vidta alla åtgärder som krävs för att säkerställa att utformningen, utvecklingen, produktionen samt processerna för sårbarhetshantering och övervakningen av dessa ska leder till att de tillverkade eller utvecklade produkterna med digitala element och de processer som tillverkaren infört överensstämmer med de väsentliga kraven i avsnitten 1 och 2 i bilaga I.

4. Märkning om överensstämmelse och försäkran om överensstämmelse

4.1. Tillverkaren ska anbringa CE-märkningen på varje enskild produkt med digitala element som uppfyller de tillämpliga kraven i denna förordning.

4.2. Tillverkaren ska upprätta en skriftlig EU-försäkran om överensstämmelse för varje produkt med digitala element i enlighet med artikel 20 och ska kunna uppvisa den tillsammans med den tekniska dokumentationen för de nationella myndigheterna under en period på 10 år efter det att produkten med digitala element har släppts ut på marknaden. I EU-försäkran om överensstämmelse ska det anges för vilken produkt med digitala element den har upprättats. En kopia av EU-försäkran om överensstämmelse ska på begäran göras tillgänglig för de relevanta myndigheterna.

5. Tillverkarens representanter

   Tillverkarens skyldigheter enligt punkt 4 får fullgöras, för dennes räkning och på dennes ansvar, av tillverkarens representant, förutsatt att dessa skyldigheter specificeras i fullmakten.

EU-typkontroll (baserat på modul B)

1. EU-typkontroll är den del av ett förfarande för bedömning av överensstämmelse genom vilken ett anmält organ undersöker en produkts tekniska utformning och utveckling och de processer för sårbarhetshantering som tillverkaren infört och intygar att en produkt med digitala element uppfyller de väsentliga kraven i avsnitt 1 i bilaga I och att tillverkaren uppfyller de väsentliga kraven i avsnitt 2 i bilaga I.

– EU-typkontroll ska göras genom bedömning av lämpligheten hos den tekniska utformningen och utvecklingen av produkten genom granskning av den tekniska

dokumentation och de underlag som avses i punkt 3 samt undersökning av provexemplar av en eller flera kritiska delar av produkten (kombination av produktionstyp och utformningstyp).

2. Tillverkaren ska lämna in ansökan om EU-typkontroll till ett valfritt anmält organ.

Ansökan ska innehålla följande:

– Tillverkarens namn och adress och, om ansökan lämnas in av tillverkarens representant, även dennes namn och adress.

– En skriftlig försäkran om att samma ansökan inte har lämnats in till något annat anmält organ.

– Den tekniska dokumentationen, vilken ska göra det möjligt att bedöma produktens överensstämmelse med de tillämpliga väsentliga kraven i avsnitt 1 i bilaga I och tillverkarens processer för sårbarhetshantering enligt avsnitt 2 i bilaga I, och ska innehålla en tillfredsställande analys och bedömning av riskerna. Den tekniska dokumentationen ska innehålla de tillämpliga kraven och, i den mån det krävs för bedömningen, även en beskrivning av produktens utformning, tillverkning och funktion. Den tekniska dokumentationen ska, i tillämpliga fall, innehålla minst de uppgifter som anges i bilaga V.

– Underlag som visar att de lösningarna för teknisk utformning och utveckling samt processerna för sårbarhetshantering är lämpliga. I underlaget ska anges alla dokument som har använts, särskilt när de relevanta harmoniserade standarderna och/eller de tekniska specifikationerna inte har tillämpats fullt ut. Underlaget ska vid behov innehålla resultaten av provningar som utförts i tillverkarens därtill ägnade laboratorium eller i något annat provningslaboratorium för dennes räkning och under dennes ansvar.

3. Det anmälda organet ska göra följande:

3.1. Granska den tekniska dokumentationen och underlaget för att bedöma om den tekniska utformningen och utvecklingen av produkten uppfyller de väsentliga kraven i avsnitt 1 i bilaga I och om de processer för sårbarhetshantering som tillverkaren infört uppfyller de väsentliga kraven i avsnitt 2 i bilaga I.

3.2. Kontrollera att provexemplaret/-aren har utvecklats eller tillverkats i enlighet med den tekniska dokumentationen och identifiera de delar som har utformats och utvecklats i enlighet med de tillämpliga bestämmelserna i de relevanta harmoniserade standarderna och/eller de tekniska specifikationerna, liksom de delar som har utformats och utvecklats utan att de tillämpliga bestämmelserna i dessa standarder har följts.

3.3. Utföra eller låta utföra lämpliga undersökningar och provningar för att, i de fall där tillverkaren har valt att tillämpa lösningarna i de relevanta harmoniserade standarderna och/eller de tekniska specifikationerna för de krav som anges i bilaga I, kontrollera att dessa lösningar har tillämpats på rätt sätt.

3.4. Utföra eller låta utföra lämpliga undersökningar och provningar för att, i de fall där lösningarna i relevanta harmoniserade standarder och/eller tekniska specifikationer för de krav som anges i bilaga I inte har tillämpats, kontrollera om de lösningar som tillverkaren använt uppfyller de väsentliga kraven.

3.5. Komma överens med tillverkaren om var undersökningarna och provningarna ska utföras.

4. Det anmälda organet ska utarbeta en bedömningsrapport i vilken de åtgärder som utförts i enlighet med punkt 4 och resultatet av dem redovisas. Utan att det påverkar det anmälda organets skyldigheter gentemot de anmälande myndigheterna får organet endast offentliggöra hela eller delar av innehållet i rapporten med tillverkarens samtycke.

5. Om typen och processerna för sårbarhetshantering uppfyller de väsentliga kraven i bilaga I ska det anmälda organet utfärda ett EU-typintyg till tillverkaren. Intyget ska innehålla tillverkarens namn och adress, slutsatserna av undersökningen, eventuella giltighetsvillkor och de uppgifter som krävs för identifiering av den godkända typen och processerna för sårbarhetshantering. Intyget kan ha en eller flera bilagor.

   Intyget och bilagorna ska innehålla all information som behövs för att bedöma om de tillverkade eller utvecklade produkterna överensstämmer med den undersökta typen och processerna för sårbarhetshantering och för att kontrollera produkter i bruk.

   Om typen och processerna för sårbarhetshantering inte uppfyller de tillämpliga väsentliga kraven i bilaga I ska det anmälda organet avslå ansökan om EU-typintyg och informera sökanden om detta samt utförligt motivera avslaget.

6. Det anmälda organet ska följa med i den tekniska utvecklingen, och om denna tyder på att den godkända typen och processerna för sårbarhetshantering inte längre uppfyller de tillämpliga väsentliga kraven i bilaga I ska organet fastställa om det krävs ytterligare undersökningar. Om så är fallet ska det anmälda organet underrätta tillverkaren om detta.

   Tillverkaren ska underrätta det anmälda organ som innehar den tekniska dokumentationen för EU-typintyget om alla ändringar av den godkända typen och processerna för sårbarhetshantering som kan påverka överensstämmelsen med de väsentliga kraven i bilaga I eller villkoren för intygets giltighet. För sådana ändringar krävs ytterligare godkännande i form av ett tillägg till det ursprungliga EU-typintyget.

7. Varje anmält organ ska underrätta sina anmälande myndigheter om de EU-typintyg och/eller tillägg till dessa som det har utfärdat eller återkallat, och det ska periodiskt återkommande eller på begäran ge de anmälande myndigheterna tillgång till förteckningen över de intyg och/eller eventuella tillägg till dessa som det har avslagit, tillfälligt återkallat eller på annat sätt belagt med restriktioner.

   Varje anmält organ ska underrätta de övriga anmälda organen om de EU-typintyg och/eller eventuella tillägg till dessa som det har vägrat utfärda, slutgiltigt eller tillfälligt återkallat eller på annat sätt belagt med restriktioner och, på begäran, om de intyg och/eller tillägg till dessa som det har utfärdat.

   Kommissionen, medlemsstaterna och de övriga anmälda organen har rätt att på begäran få en kopia av EU-typkontrollintyget och/eller tillägg till det. Kommissionen och medlemsstaterna har rätt att på begäran få en kopia av den tekniska dokumentationen och av resultaten från de undersökningar som utförts av det anmälda organet. Det anmälda organet ska spara en kopia av EU-typintyget med bilagor och tillägg samt av den tekniska dokumentationen, inklusive dokumentation från tillverkaren, så länge som intyget är giltigt.

8. Tillverkaren ska för de nationella myndigheterna kunna uppvisa en kopia av EU-typintyget med bilagor och tillägg tillsammans med den tekniska dokumentationen under tio år efter det att produkten släpptes ut på marknaden.

9. Tillverkarens representant får lämna in den ansökan som avses i punkt 3 och fullgöra skyldigheterna enligt punkterna 7 och 9, förutsatt att skyldigheterna specificeras i fullmakten.

Överensstämmelse med typ som grundar sig på intern tillverkningskontroll (baserat på modul C)

1. Överensstämmelse med typ som grundar sig på intern tillverkningskontroll är den del av ett förfarande för bedömning av överensstämmelse genom vilken tillverkaren fullgör skyldigheterna i punkterna 2 och 3 samt säkerställer och försäkrar att de berörda produkterna överensstämmer med typen enligt beskrivningen i EU-typintyget och uppfyller de väsentliga kraven i avsnitt 1 i bilaga I.

2. Produktion

2.1. Tillverkaren ska vidta alla nödvändiga åtgärder för att produktionen och övervakningen av den ska leda till att de tillverkade produkterna överensstämmer med den godkända typen enligt beskrivningen i EU-typintyget och med de väsentliga kraven i avsnitt 1 i bilaga I.

3. Märkning om överensstämmelse och försäkran om överensstämmelse

3.1. Tillverkaren ska anbringa CE-märkningen på varje enskild produkt som överensstämmer med typen enligt beskrivningen i EU-typintyget och uppfyller de tillämpliga kraven i lagstiftningsintrumentet.

3.2. Tillverkaren ska upprätta en skriftlig försäkran om överensstämmelse för en produktmodell och kunna uppvisa den för de nationella myndigheterna under en period på tio år efter det att produkten har släppts ut på marknaden. I försäkran om överensstämmelse ska det anges för vilken produktmodell den har upprättats. En kopia av försäkran om överensstämmelse ska på begäran göras tillgänglig för de behöriga myndigheterna.

4. Tillverkarens representant

Tillverkarens skyldigheter enligt punkt 3 får fullgöras, för dennes räkning och på dennes ansvar, av tillverkarens representant, förutsatt att skyldigheterna anges i fullmakten.

Överensstämmelse som grundar sig på fullständig kvalitetssäkring (baserat på modul H)

1. Överensstämmelse som grundar sig på fullständig kvalitetssäkring är det förfarande för bedömning av överensstämmelse genom vilket tillverkaren fullgör skyldigheterna i punkterna 2 och 5 samt säkerställer och försäkrar på eget ansvar att de berörda produkterna (eller produktkategorierna) uppfyller de väsentliga kraven i avsnitt 1 i bilaga I och att de processer för sårbarhetshantering som tillverkaren infört uppfyller kraven i avsnitt 2 i bilaga I.

2. Utformning, utveckling, produktion och sårbarhetshantering av produkter med digitala element

Tillverkaren ska tillämpa ett godkänt kvalitetssystem enligt punkt 3 för utformning, utveckling och produktion av de berörda produkterna och för hantering av sårbarheter, upprätthålla dess effektivitet under de berörda produkternas hela livscykel och ska stå under övervakning i enlighet med punkt 4.

3. Kvalitetssystem

3.1. Tillverkaren ska hos ett valfritt anmält organ ansöka om att få sitt kvalitetssystem för de berörda produkterna bedömt.

Ansökan ska innehålla följande:

– Tillverkarens namn och adress och, om ansökan lämnas in av tillverkarens representant, även dennes namn och adress.

– Den tekniska dokumentationen för en modell av varje kategori av produkter som är tänkt att tillverkas eller utvecklas. Den tekniska dokumentationen ska, i tillämpliga fall, innehålla de uppgifter som anges i bilaga V.

– Dokumentation av kvalitetssystemet.

– En skriftlig försäkran om att samma ansökan inte har lämnats till något annat anmält organ.

3.2. Kvalitetssystemet ska säkerställa att produkterna uppfyller de väsentliga kraven i avsnitt 1 i bilaga I och att de processer för sårbarhetshantering som tillverkaren infört uppfyller kraven i avsnitt 2 i bilaga I.

Alla de faktorer, krav och bestämmelser som tillverkaren tagit hänsyn till ska dokumenteras på ett systematiskt och överskådligt sätt i form av skriftliga riktlinjer, förfaranden och anvisningar. Denna dokumentation av kvalitetssystemet ska möjliggöra en enhetlig tolkning av rutiner och kvalitetsåtgärder, såsom program, planer, manualer och protokoll.

Den ska framför allt innehålla en fullgod beskrivning av

– kvalitetsmålen och organisationsstruktur samt ledningens ansvar och befogenheter när det gäller utformning, utveckling, produktkvalitet och sårbarhetshantering,

– de tekniska specifikationer för utformning och utveckling, inklusive standarder, som ska tillämpas och, när de relevanta harmoniserade standarderna eller de tekniska föreskrifterna inte tillämpas fullt ut, de medel som används för att säkerställa att de väsentliga kraven i avsnitt 1 i bilaga I som gäller för produkterna uppfylls,

– de tekniska specifikationer för förfaranden, inklusive standarder, som ska tillämpas och, när de relevanta harmoniserade standarderna eller de tekniska föreskrifterna inte tillämpas fullt ut, de medel som används för att säkerställa att de väsentliga kraven i avsnitt 2 i bilaga I som gäller för tillverkaren uppfylls,

– kontrollen av utformning och utveckling, samt de metoder, processer och systematiska förfaranden för verifikation av utformning och utveckling som ska användas vid utformning och utveckling av produkter inom den berörda kategorin,

– de motsvarande metoder, processer och systematiska åtgärder för produktion, kvalitetskontroll och kvalitetssäkring som ska användas,

– de undersökningar och provningar som kommer att utföras före, under och efter produktionen, och hur ofta de kommer att utföras,

– kvalitetsdokumenten, t.ex. kontrollrapporter och provningsresultat, kalibreringsresultat och redogörelser för den berörda personalens kvalifikationer,

– metoderna för övervakning av att den erforderliga utformnings- och produktkvaliteten uppnås och att kvalitetssystemet fungerar effektivt.

3.3. Det anmälda organet ska bedöma kvalitetssystemet för att avgöra det uppfyller kraven i punkt 3.2.

Det ska förutsätta att kraven är uppfyllda i fråga om de delar av kvalitetssäkringssystemet som uppfyller motsvarande specifikationer i den nationella standard genom vilken den relevanta harmoniserade standarden och/eller de tekniska specifikationerna genomförs.

Utöver erfarenhet av kvalitetsledningssystem ska minst en av revisionsgruppens deltagare ha erfarenhet av bedömning av det aktuella produktområdet och den berörda produkttekniken, och känna till de tillämpliga kraven i denna förordning. Revisionen ska även omfatta ett bedömningsbesök i tillverkarens anläggning, om en sådan anläggning finns. Revisionsgruppen ska granska den tekniska dokumentation som avses i punkt 3.1 andra strecksatsen för att kontrollera att tillverkaren känner till de tillämpliga kraven i denna förordning och kan utföra de undersökningar som krävs för att säkerställa att produkten överensstämmer med kraven.

Tillverkaren eller dennes representant ska meddelas beslutet.

Meddelandet ska innehålla slutsatserna från revisionen och det motiverade bedömningsbeslutet.

3.4. Tillverkaren ska åta sig att fullgöra de skyldigheter som är förenade med det godkända kvalitetssystemet och att upprätthålla det så att det förblir ändamålsenligt och effektivt.

3.5. Tillverkaren ska informera det anmälda organ som har godkänt kvalitetssystemet om alla planerade ändringar av systemet.

Det anmälda organet ska bedöma de föreslagna ändringarna och avgöra om ett ändrat kvalitetssystem fortfarande uppfyller de krav som avses i punkt 3.2 eller om en ny bedömning är nödvändig.

Det ska meddela tillverkaren sitt beslut. Meddelandet ska innehålla slutsatserna från undersökningen och det motiverade bedömningsbeslutet.

4. Övervakning under det anmälda organets ansvar

4.1. Syftet med övervakningen är att säkerställa att tillverkaren fullgör de skyldigheter som är förenade med det godkända kvalitetssystemet.

4.2. För att möjliggöra en bedömning ska tillverkaren ge det anmälda organet tillträde till lokaler för utformning, utveckling, produktion, kontroll, provning och lagring och tillhandahålla all nödvändig information, särskilt i fråga om

– dokumentationen av kvalitetssystemet,

– de dokument som anges i kvalitetssystemets utformningsdel, t.ex. resultat från analyser, beräkningar och provningar,

– de dokument som anges i kvalitetssystemets tillverkningsdel, t.ex. kontrollrapporter, provningsresultat, kalibreringsresultat och redogörelser för den berörda personalens kvalifikationer.

4.3. Det anmälda organet ska regelbundet genomföra revisioner för att säkerställa att tillverkaren vidmakthåller och tillämpar kvalitetssystemet, samt överlämna en revisionsrapport till tillverkaren.

5. Märkning om överensstämmelse och försäkran om överensstämmelse

5.1. Tillverkaren ska anbringa CE-märkningen och, under ansvar av det anmälda organ som avses i punkt 3.1, organets identifikationsnummer på varje enskild produkt som uppfyller kraven i avsnitt 1 i bilaga I till denna förordning.

5.2. Tillverkaren ska upprätta en skriftlig försäkran om överensstämmelse för en produktmodell och kunna uppvisa den för de nationella myndigheterna under en period på tio år efter det att produkten har släppts ut på marknaden. I försäkran om överensstämmelse ska det anges för vilken produktmodell den har upprättats.

En kopia av försäkran om överensstämmelse ska på begäran göras tillgänglig för de behöriga myndigheterna.

6. Tillverkaren ska under en period på minst tio år efter det att produkten har släppts ut på marknaden kunna uppvisa följande för de nationella myndigheterna:

– Den tekniska dokumentation som avses i punkt 3.1.

– Sådan dokumentation av kvalitetssystemet som avses i punkt 3.1.

– Godkända ändringar som avses i punkt 3.5.

– De beslut och rapporter från det anmälda organet som avses i punkterna 3.5, 4.3 och 4.4.

7. Varje anmält organ ska underrätta sina anmälande myndigheter om de godkännanden av kvalitetssystem som det har utfärdat eller återkallat och ska regelbundet eller på begäran ge de anmälande myndigheterna tillgång till förteckningen över godkännanden som det har vägrat att utfärda, tillfälligt återkallat eller på annat sätt belagt med restriktioner.

Varje anmält organ ska underrätta de övriga anmälda organen om de godkännanden av kvalitetssystem som det har vägrat utfärda eller tillfälligt eller slutgiltigt återkallat och, på begäran, om de godkännanden av kvalitetssystem som det har utfärdat.

8. Tillverkarens representant

Tillverkarens skyldigheter enligt punkterna 3.1, 3.5, 5 och 6 får fullgöras, för dennes räkning och på dennes ansvar, av tillverkarens representant, förutsatt att dessa skyldigheter specificeras i fullmakten.

EUROPEISKA
KOMMISSIONEN

Bryssel den 15.9.2022
COM(2022) 454 final

2022/0272 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordning (EU) 2019/1020

(Text av betydelse för EES)

{SEC(2022) 321 final} - {SWD(2022) 282 final} - {SWD(2022) 283 final}

MOTIVERING

1. BAKGRUND TILL FÖRSLAGET

• Motiv och syfte med förslaget

Hårdvaru- och programvaruprodukter utsätts allt oftare för framgångsrika cyberattacker, vilket innebär att den globala årskostnaden för cyberbrottslighet beräknas uppgå till 5,5 biljoner euro 2021. Dessa produkter har två stora problem som ökar kostnaderna för användarna och för samhället: 1) en låg cybersäkerhetsnivå, vilket visas av utbredda sårbarheter och ett otillräckligt och inkonsekvent tillhandahållande av säkerhetsuppdateringar som åtgärdar dessa sårbarheter, samt 2) brister i användarnas förståelse och tillgång till information, vilket hindrar dem från att välja produkter med tillfredsställande cybersäkerhetsegenskaper eller använda dem på ett säkert sätt. I en uppkopplad miljö kan en cybersäkerhetsincident hos en produkt påverka en hel organisation eller en hel leveranskedja, och ofta sprida sig över gränserna på den inre marknaden på bara några minuter. Detta kan leda till allvarliga störningar av ekonomisk och samhällelig verksamhet och till och med bli livshotande.

Cybersäkerheten för produkter med digitala element har en stark gränsöverskridande dimension, eftersom produkter som tillverkas i ett land ofta används på hela den inre marknaden. Det är också vanligt att incidenter som först påverkar en enda enhet eller en enda medlemsstat sprids till hela den inre marknaden på bara några få minuter.

Den befintliga inremarknadslagstiftningen omfattar visserligen vissa produkter med digitala element, men de flesta hårdvaru- och programvaruprodukter omfattas i dagsläget inte av någon cybersäkerhetslagstiftning på EU-nivå. EU:s nuvarande rättsliga ram behandlar inte cybersäkerheten för icke-inbyggd programvara, trots att cybersäkerhetsattacker allt oftare riktas mot sårbarheter i sådana produkter, vilket medför stora samhälleliga och ekonomiska kostnader. Det finns många exempel på anmärkningsvärda cyberattacker som beror på bristfällig produktsäkerhet, såsom gisslanmasken WannaCry, som utnyttjade en sårbarhet i Windows som 2017 påverkade 200 000 datorer i 150 länder och orsakade skador som uppgick till miljarder US-dollar, leveranskedjeattacken mot Kaseya VSA, där man använde Kaseyas nätförvaltningsprogram för att attackera över 1 000 företag och tvinga en butikskedja att stänga alla sina 500 butiker i Sverige, eller de många incidenter där bankappar hackas och syftet är att stjäla pengar från intet ont anande kunder.

Två huvudmål identifierades för att säkerställa en korrekt fungerande inre marknad: 1) att skapa rätt förutsättningar för utvecklingen av säkra produkter med digitala element genom att säkerställa att hårdvaru- och programvaruprodukter har färre sårbarheter när de släpps ut på marknaden och att tillverkarna tar säkerheten på allvar under produktens hela livscykel, och 2) att skapa förutsättningar för att användarna ska kunna ta hänsyn till cybersäkerheten när de väljer och använder produkter med digitala element. Fyra särskilda mål fastställdes: i) att säkerställa att tillverkarna förbättrar säkerheten för produkter med digitala element från utformnings- och utvecklingsfasen och genom hela produktens livscykel, ii) att säkerställa en sammanhängande cybersäkerhetsram, som främjar överensstämmelse för hårdvaru- och programvaruproducenter, iii) att förbättra transparensen när det gäller säkerhetsegenskaperna hos produkter med digitala element, och iv) att möjliggöra en säker användning av produkter med digitala element för företag och konsumenter.

Cybersäkerhetens starka gränsöverskridande dimension och det ökande antalet incidenter, med spridningseffekter över gränser och mellan sektorer och produkter innebär att målen inte

kan uppnås på ett effektivt sätt av medlemsstaterna på egen hand. Eftersom marknaderna för produkter med digitala element är globala möter alla medlemsstater samma risker för samma produkter med digitala element på sina territorier. En framväxande fragmenterad ram bestående av potentiellt varierande nationella regler riskerar att stå i vägen för en öppen och konkurrenspräglad inre marknad för produkter med digitala element. Det krävs alltså gemensamma åtgärder på EU-nivå för att öka förtroendet hos användarna och stärka dragningskraften för EU-produkter med digitala element. Detta skulle också gagna den inre marknaden genom att skapa rättssäkerhet och lika spelregler för alla säljare av produkter med digitala element, vilket också visas i slutrapporten från konferensen om Europas framtid, där medborgarna efterlyste en starkare roll för EU i arbetet mot cybersäkerhetshot.

- **Samspel med befintliga bestämmelser inom området**

EU-ramen består av övergripande lagstiftning med rättsakter som täcker vissa cybersäkerhetsaspekter ur olika vinklar (produkter, tjänster, krishantering och brottslighet). År 2013 trädde direktivet om angrepp mot informationssystem[1] i kraft, och det harmoniserade kriminalisering och påföljder för ett antal brott riktade mot informationssystem. I augusti 2016 trädde direktiv (EU) 2016/1148 om säkerhet i nätverks- och informationssystem (NIS-direktivet)[2] i kraft som den första rättsakten i en EU-täckande cybersäkerhetslagstiftning. Översynen av det direktivet resulterade i direktiv [direktiv XXX/XXXX (NIS2)], som höjer den gemensamma ambitionsnivån i EU. År 2019 trädde EU:s cybersäkerhetsakt[3] i kraft. Den syftar till att förbättra säkerheten för IKT-produkter, IKT-tjänster och IKT-processer genom att införa en frivillig europeisk ram för cybersäkerhetscertifiering[4].

För att cybersäkerhet ska kunna säkerställas i hela leveranskedjan måste alla ingående komponenter vara cybersäkra. I detta hänseende finns det dock stora luckor i den nämnda EU-lagstiftningen, eftersom den inte omfattar obligatoriska krav för säkerheten i produkter med digitala element.

Medan förslaget omfattar produkter med digitala element som släpps ut på marknaden syftar direktiv [direktiv XXX/XXX (NIS2)] till att säkerställa en hög cybersäkerhetsnivå för tjänster som tillhandahålls av väsentliga och viktiga entiteter. Enligt direktiv [direktiv XXX/XXXX (NIS2)] ska medlemsstaterna säkerställa att de väsentliga och viktiga entiteter som omfattas, såsom vårdleverantörer, molnleverantörer och offentliga förvaltningar, vidtar ändamålsenliga och proportionella tekniska, operativa och organisatoriska cybersäkerhetsåtgärder. Detta innefattar bland annat ett krav på att säkerställa säkerheten vid förvärv, utveckling och underhåll av nätverks- och informationssystem, inbegripet hantering av och information om sårbarheter. Enligt direktiv [direktiv XXX/XXXX (NIS2)] ska kommissionen anta genomförandeakter för att fastställa teknik- och metodkraven för dessa åtgärder inom 21 månader från direktivets ikraftträdande för vissa typer av entiteter, såsom leverantörer av

---

1 Europaparlamentets och rådets direktiv 2013/40/EU av den 12 augusti 2013 om angrepp mot informationssystem och om ersättande av rådets rambeslut 2005/222/RIF (EUT L 218, 14.8.2013, s. 8).

2 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 (EUT L 194, 19.7.2016, s. 1).

3 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).

4 Cybersäkerhetsakten gör det möjligt att utveckla särskilda certifieringssystem. Varje system omfattar hänvisningar till relevanta standarder, tekniska specifikationer eller andra cybersäkerhetskrav som fastställs inom systemet. Beslutet om att utveckla en cybersäkerhetscertifiering är riskbaserat.

molntjänster. För alla andra entiteter får kommissionen anta en genomförandeakt för att fastställa teknik-, metod- och sektorskrav. Denna ram kommer att säkerställa att tekniska specifikationer och åtgärder som liknar de väsentliga cybersäkerhetskraven enligt cyberresiliensakten också genomförs i samband med utformningen, utvecklingen och sårbarhetshanteringen av programvara som tillhandahålls i form av en tjänst (*Software-as-a-Service, SaaS*). Detta skulle kunna vara ett sätt att säkerställa en hög cybersäkerhetsnivå exempelvis för elektroniska patientjournalsystem, även när sådana levereras som nättjänster (SaaS) eller utvecklas av hälso- och sjukvårdsinstitutionerna själva (in-house), i enlighet med den föreslagna [förordningen om ett europeiskt hälsodataområde].

- **Samspel med unionens politik inom andra områden**

Såsom anges i meddelandet *Att forma EU:s digitala framtid*[5] är det av avgörande betydelse för EU att ta till vara alla möjligheter som den digitala tidsåldern erbjuder för att inom säkra och etiska gränser stärka sin industri och innovationsförmåga. I EU-strategin för data fastställs fyra pelare – dataskydd, grundläggande rättigheter, säkerhet och cybersäkerhet – var och en av dem en nödvändig förutsättning för att ett samhälle ska kunna stärkas genom användning av data.

Den nuvarande EU-ramen[6] för produkter som också kan ha digitala element återfinns i flera olika rättsakter, bland annat EU-lagstiftning om specifika produkter vilka omfattar säkerhetsrelaterade aspekter samt allmän lagstiftning om produktansvar. Förslaget är förenligt med EU:s nuvarande produktrelaterade regelverk samt med nyare lagstiftningsförslag såsom kommissionens förslag till förordning [förordningen om artificiell intelligens (AI)][7].

Den föreslagna förordningen är avsedd att tillämpas på all radioutrustning som omfattas av kommissionens delegerade förordning (EU) 2022/30. De krav som fastställs i denna förordning omfattar alla aspekter av de väsentliga krav som avses i artikel 3.3 d, e och f i direktiv 2014/53/EU, inbegripet de viktigaste aspekter som fastställs i [kommissionens genomförandebeslut XXX/2022 om en begäran om standardisering till europeiska standardiseringsorganisationer] som utfärdats på grundval av den delegerade förordningen. För att undvika överlappningar i lagstiftningen är planen att kommissionen ska upphäva eller ändra den delegerade förordningen vad gäller radioutrustning som omfattas av den föreslagna förordningen, så att det är den senare som gäller när den börjar tillämpas.

För att undvika dubbelarbete ska också kommissionen och de europeiska standardiseringsorganisationerna ta hänsyn till det standardiseringsarbete som gjorts inom ramen för kommissionens genomförandebeslut C(2022)5637 om en begäran om standardisering för delegerad förordning 2022/30 i samband med förberedelserna och utarbetandet av harmoniserade standarder för att underlätta genomförandet av förordningen.

---

5 Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén, *Att forma EU:s digitala framtid*, COM(2020) 67 final av den 19 februari 2020.

6 I första hand lagstiftning inom den nya lagstiftningsramen.

7 Förslag till Europaparlamentets och rådets förordning om harmoniserade regler för artificiell intelligens (rättsakt om artificiell intelligens) och om ändring av vissa unionslagstiftningsakter av den 21 april 2021 (COM(2021) 206 final).

2. RÄTTSLIG GRUND, SUBSIDIARITETSPRINCIPEN OCH PROPORTIONALITETSPRINCIPEN

• Rättslig grund

Den rättsliga grunden för förslaget är artikel 114 i förslaget om Europeiska unionens funktionssätt (*EUF-fördraget*), där det föreskrivs att det ska beslutas om åtgärder för att säkerställa upprättandet av den inre marknaden och dess funktion. Syftet med förslaget är att harmonisera cybersäkerhetskraven för produkter med digitala element i alla medlemsstater och att avskaffa hinder för den fria rörligheten för varor.

Artikel 114 i EUF-fördraget kan användas som rättslig grund för att förhindra att dessa hinder uppstår till följd av skillnader i nationell lagstiftning och nationella metoder för att hantera rättsliga oklarheter och luckor i de befintliga rättsliga ramarna[8]. Domstolen har också bekräftat att tillämpning av olikartade tekniska krav kan vara en giltig grund för att utlösa artikel 114 i EUF-fördraget[9].

EU:s nuvarande lagstiftningsram för produkter med digitala element baseras på artikel 114 i EUF-fördraget och omfattar flera rättsakter, bland annat om specifika produkter och säkerhetsrelaterade aspekter eller allmän lagstiftning om produktansvar. Den täcker dock endast vissa aspekter som är kopplade till cybersäkerheten för fysiska digitala produkter och, i förekommande fall, programvara som ingår i dessa produkter. På nationell nivå börjar medlemsstaterna vidta nationella åtgärder som ålägger försäljare av digitala produkter att förbättra cybersäkerheten[10]. Samtidigt har cybersäkerheten för digitala produkter en särskilt stark gränsöverskridande dimension, eftersom produkter som tillverkas i ett land ofta används av organisationer och konsumenter på hela den inre marknaden. Det är vanligt att incidenter som först påverkar en enda enhet eller medlemsstat sprider sig till hela organisationer, sektorer och andra medlemsstater på bara några minuter.

De olika rättsakter och initiativ som hittills har vidtagits på EU-nivå och nationell nivå åtgärdar endast delvis de identifierade problemen och riskerar att ge upphov till ett lapptäcke av lagar på den inre marknaden och öka rättsosäkerheten för både försäljare och användare av dessa produkter. Det kan också bli onödigt betungande för företag att behöva uppfylla många olika krav för samma typer av produkter.

Den föreslagna förordningen skulle harmonisera och rationalisera EU:s regelverk genom att införa cybersäkerhetskrav för produkter med digitala element och motverka överlappande krav till följd av olika rättsakter. Detta ökar rättssäkerheten för aktörer och användare i hela unionen och ökar harmoniseringen på den europeiska inre marknaden, vilket skapar hållbara villkor för aktörer som vill komma in på EU-marknaden.

• Subsidiaritetsprincipen (för icke-exklusiv befogenhet)

Cybersäkerhetens generellt starka gränsöverskridande dimension och det ökande antalet risker och incidenter, med spridningseffekter över gränser och mellan sektorer och produkter, innebär att målen för denna åtgärd inte kan uppnås på ett effektivt sätt av medlemsstaterna på

---

8 Domstolens dom (stora avdelningen) av den 3 december 2019. Tjeckiska republiken mot Europaparlamentet och Europeiska unionens råd, mål C-482/17, punkt 35.

9 Domstolens dom (stora avdelningen) den 2 maj 2006. Förenade konungariket Storbritannien och Nordirland mot Europaparlamentet och Europeiska unionens råd, mål C-217/04, punkterna 62–63.

10 Exempelvis införde Finland 2019 ett märkningssystem för sakernas internet (t.ex. smart-tv, smartmobiler och leksaker) baserat på Etsi-standarder. Tyskland har nyligen infört en konsumentsäkerhetsmärkning för bredbandsroutrar, smart-tv, kameror, högtalare, leksaker och rengörings- och trädgårdsrobotar.

egen hand. Nationella strategier för att hantera problemen, i synnerhet strategier som omfattar obligatoriska krav, kommer att öka rättsosäkerheten och de rättsliga hindren. Företagen kan hindras från en sömlös expansion till andra medlemsstater, vilket innebär att användarna berövas produkternas fördelar.

Det krävs alltså gemensamma åtgärder på EU-nivå för att säkra en hög nivå av förtroende hos användarna och stärka dragningskraften för EU-produkter med digitala element. Detta skulle samtidigt gagna den digitala inre marknaden och den inre marknaden i allmänhet genom att skapa rättssäkerhet och säkra lika spelregler för alla tillverkare av produkter med digitala element.

I rådets slutsatser av den 23 maj 2022 om utveckling av Europeiska unionens arbete på cyberområdet uppmanas kommissionen att före utgången av 2022 lägga fram förslag om gemensamma cybersäkerhetskrav för uppkopplade enheter.

- **Proportionalitetsprincipen**

När det gäller proportionaliteten för den föreslagna förordningen skulle åtgärderna i de undersökta alternativen inte gå utöver vad som är nödvändigt för att uppnå de allmänna och särskilda målen och skulle inte medföra några oproportionerliga kostnader. Åtgärden skulle säkerställa att produkter med digitala element görs säkra under hela sin livscykel och den skulle stå i proportion till riskerna genom målinriktade och teknikneutrala krav som förblir rimliga och allmänt sett motsvarar de berörda enheternas intressen.

De väsentliga cybersäkerhetskraven i förslaget bygger på allmänt använda standarder och den därpå följande standardiseringsprocessen skulle ta hänsyn till produkternas tekniska särdrag. Detta innebär att säkerhetskontrollerna anpassas när det behövs för en viss risknivå. De planerade övergripande reglerna skulle endast omfatta tredjepartsbedömningar när det gäller kritiska produkter, som endast utgör ett begränsat segment av marknaden för produkter med digitala element. Åtgärdens inverkan på små och medelstora företag skulle bero på i vilken mån som de finns på marknaden för dessa specifika produktkategorier.

När det gäller proportionaliteten för kostnaderna för bedömning av överensstämmelse skulle anmälda organ som genomför tredjepartsbedömningarna ta hänsyn till företagets storlek när de fastställer avgiften. En rimlig övergångsperiod på 24 månader skulle också ges för att förbereda genomförandet, ge de berörda marknaderna tid att förbereda sig och samtidigt tydligt visa riktningen för investeringar i forskning och utveckling. Företagens kostnader för att uppfylla kraven skulle uppvägas av vinsterna genom en högre säkerhetsnivå för produkter med digitala element och i förlängningen öka användarnas förtroende för dessa produkter.

- **Val av instrument**

En lagstiftningsåtgärd skulle innebära antagandet av en förordning och inte av ett direktiv. Anledningen är att för denna specifika typ av produktlagstiftning skulle en förordning åtgärda de identifierade problemen och uppnå de angivna målen på ett mer effektivt sätt, eftersom det är en åtgärd som fastställer villkor för utsläppandet på den inre marknaden för en väldigt bred produktkategori. För en sådan åtgärd skulle ett direktivs införlivandeprocess lämna ett alltför stort utrymme för avgöranden på nationell nivå, vilket kan leda till bristande enhetlighet för vissa väsentliga cybersäkerhetskrav och till rättsosäkerhet, fortsatt fragmentering och till och med diskrimineringssituationer över gränser, i synnerhet med tanke på att de produkter som omfattas kan ha flera olika syften eller användningsområden och att tillverkare kan producera många olika kategorier av sådana produkter.

3. RESULTAT AV EFTERHANDSUTVÄRDERINGAR, SAMRÅD MED BERÖRDA PARTER OCH KONSEKVENSBEDÖMNINGAR

- **Samråd med berörda parter**

Kommissionen har samrått med ett brett spektrum av berörda parter. Medlemsstaterna och berörda parter inbjöds till att delta i det öppna offentliga samrådet och i de enkäter och workshoppar som anordnades i samband med den studie som gjordes av ett konsortium som underlag för kommissionens förberedande arbete inför konsekvensbedömningen. Wavestone, Centre for European Policy Studies (CEPS) och ICF. Deltagarna var bl.a. nationella marknadskontrollmyndigheter, unionsorgan som arbetar med cybersäkerhetsfrågor, hårdvaru- och programvarutillverkare, importörer och distributörer av hårdvara och programvara, branschorganisationer, konsumentorganisationer och användare av produkter med digitala element, medborgare, forskare, den akademiska världen, anmälda organ och ackrediteringsorgan samt yrkesfolk från cybersäkerhetsbranschen.

Samråden omfattade följande:

- En första studie, som genomfördes av ett konsortium bestående av ICF, Wavestone, Carsa och CEPS, och som lades fram i december 2021[11]. I studien identifierades flera marknadsmisslyckanden och granskades tänkbara regleringsåtgärder.
- Ett öppet offentligt samråd som riktades till medborgare, intressenter och cybersäkerhetsexperter. 176 svar inkom. På så sätt fick man in en mängd olika synpunkter och erfarenheter från alla intressentgrupper.
- Workshoppar anordnades inom ramen för studien till stöd för kommissionens förberedande arbete för en cyberresiliensakt. De samlade omkring 100 deltagare från samtliga 27 medlemsstater och många olika intressenter företräddes.
- Man gjorde intervjuer med experter för att få en fördjupad förståelse av de aktuella cybersäkerhetsutmaningarna i samband med produkter med digitala element och diskutera alternativen för en eventuell regleringsåtgärd.
- Bilaterala diskussioner hölls med nationella cybersäkerhetsmyndigheter, den privata sektorn och konsumentorganisationer.
- Utåtriktad verksamhet genomfördes mot centrala intressenter från små och medelstora företag.

- **Insamling och användning av sakkunnigutlåtanden**

Samrådsverksamheten syftade till att få in synpunkter på de fem huvudutvärderingskriterierna baserat på EU:s riktlinjer för bättre lagstiftning (ändamålsenlighet, effektivitet, relevans, enhetlighet, EU-mervärde) samt de potentiella effekterna av de tänkbara alternativen för framtiden. Uppdragstagaren har inte bara vänt sig till intressenter som skulle påverkas direkt av den föreslagna förordningen utan även konsulterat en mängd experter på cybersäkerhetsområdet.

[11] *Study on the need of Cybersecurity requirements for ICT products – No. 2020-0715, Final Study Report*, finns på https://digital-strategy.ec.europa.eu/en/library/study-need-cybersecurity-requirements-ict-products.

- **Konsekvensbedömning**

Kommissionen gjorde en konsekvensbedömning för detta förslag som granskades av kommissionens nämnd för lagstiftningskontroll. Ett möte i nämnden, som hölls den 6 juli 2022, mynnade ut i ett positivt utlåtande. Konsekvensbedömningen anpassades till nämndens rekommendationer och synpunkter.

Kommissionen undersökte olika politiska alternativ för att uppnå förslagets allmänna mål.

- Ett ”icke-bindande” tillvägagångssätt och frivilliga åtgärder (alternativ 1): Detta alternativ omfattar inga obligatoriska regleringsåtgärder. Kommissionen skulle istället utfärda meddelanden, riktlinjer, rekommendationer och eventuellt uppförandekoder för att uppmuntra frivilliga åtgärder. Nationella ordningar, frivilliga eller obligatoriska, skulle även i fortsättningen utvecklas för att kompensera bristen på övergripande EU-regler.
- Ad hoc-regleringsåtgärder för cybersäkerhet för fysiska produkter med digitala element och respektive inbyggd programvara (alternativ 2): Detta alternativ skulle innefatta en produktspecifik ad hoc-regleringsåtgärd som skulle vara begränsad till tillägg till och/eller ändring av de cybersäkerhetskrav som finns i befintlig lagstiftning eller införande av ny lagstiftning när nya risker uppstår, inbegripet potentiellt för icke-inbyggd programvara.

Alternativ 3 och 4 omfattar en övergripande regleringsåtgärd av varierande omfattning, som i stort är i enlighet med den nya lagstiftningsramen. Den nya lagstiftningsramen omfattar väsentliga krav som ett villkor för utsläppande av vissa produkter på den inre marknaden. Den nya lagstiftningsramen föreskriver normalt också bedömning av överensstämmelse, alltså den process som tillverkaren genomför för att visa att särskilda produktkrav har uppfyllts.

- Ett blandat tillvägagångssätt, som innefattar övergripande obligatoriska krav för cybersäkerheten för materiella produkter som omfattar digitala element och respektive inbyggd programvara och ett stegvist tillvägagångssätt för icke-inbyggd programvara (alternativ 3): Detta alternativ skulle innebära en förordning som inför övergripande cybersäkerhetskrav för alla materiella produkter med digitala element och den programvara som ingår i dessa, som ett villkor för utsläppande på marknaden, och skulle även innefatta två underalternativ med respektive utan tredjepartsbedömning (3i och 3ii). Icke-inbyggd programvara skulle inte regleras.
- En övergripande regleringsåtgärd som omfattar cybersäkerhetskrav för ett brett spektrum av materiella och immateriella produkter med digitala element, inklusive icke-inbyggd programvara (alternativ 4): Detta alternativ liknar alternativ 3, förutom när det gäller tillämpningsområdet. Alternativ 4 skulle inkludera icke-inbyggd programvara (med två underalternativ som innebär att endast kritisk programvara (4a) respektive all programvara (4b) inkluderas) inom ramen för en eventuell förordning. För varje underalternativ skulle samma underalternativ avseende bedömning av överensstämmelse övervägas som för alternativ 3.

Alternativ 4 (med underalternativ som omfattar all programvara och involverar obligatorisk tredjepartsbedömning för kritiska produkter) utkristalliserade sig som det rekommenderade alternativet baserat på effektiviteten i förhållande till de särskilda målen och vad gäller kostnader och nytta. Detta alternativ skulle säkerställa att särskilda övergripande cybersäkerhetskrav fastställdes för alla produkter med digitala element som släpps ut eller

tillhandahålls på den inre marknaden, och det skulle vara det enda alternativ som omfattar hela den digitala leveranskedjan. Även icke-inbyggd programvara, som ofta är exponerad för sårbarheter, skulle omfattas av en sådan regleringsåtgärd, vilket därmed säkerställer en enhetlig strategi för alla produkter med digitala element, med en tydlig ansvarsfördelning mellan olika ekonomiska aktörer.

Detta alternativ ger också ett mervärde genom att omfatta aktsamhetskrav och livscykelaspekter efter utsläppandet på marknaden av produkter med digitala element, för att bland annat säkerställa ändamålsenlig information om säkerhetsstöd och tillhandahållande av säkerhetsuppdateringar. Alternativet skulle också utgöra det effektivaste komplementet till den nyligen gjorda översynen av NIS-ramen, genom att säkerställa rätt villkor för en stärkt säkerhet i leveranskedjan.

Det rekommenderade alternativet skulle innebära betydande fördelar för de olika intressenterna. För företagen skulle det förhindra att olikartade säkerhetsregler gäller för produkter med digitala element, och det skulle sänka kostnaderna för uppfyllande av kraven i cybersäkerhetslagstiftningen. Det skulle minska antalet cyberincidenter, kostnaden för incidenthantering och risken för skadat anseende. För EU som helhet beräknas att initiativet kan minska kostnaderna för incidenter som påverkar företag med i storleksordningen 180–290 miljarder euro per år. Det skulle leda till ökad omsättning tack vare en ökad efterfrågan på produkter med digitala element. Det skulle förbättra företagens globala anseende och leda till en ökad efterfrågan också utanför EU. För användarna skulle det rekommenderade alternativet öka transparensen för säkerhetsegenskaper och underlätta användningen av produkter med digitala element. Konsumenter och medborgare skulle också gagnas av ett bättre skydd för sina grundläggande rättigheter, såsom personlig integritet och skydd av personuppgifter.

Deltagarna i det offentliga samrådet ombads rangordna de olika åtgärdernas effektivitet och de var eniga om att alternativ 4 skulle vara den mest ändamålsenliga åtgärden (4,08 på en skala från 1 till 5). Detta innefattar konsumentorganisationer (5,00), deltagare som identifierar sig som användare (4,22), anmälda organ (4,17), marknadskontrollmyndigheter (5,00) och tillverkare av produkter med digitala element (3,85), inbegripet tillverkare som är små och medelstora företag (4,05).

- **Lagstiftningens ändamålsenlighet och förenkling**

Detta förslag omfattar krav som kommer att gälla för tillverkare av hårdvara och programvara. Man måste säkerställa rättssäkerheten och motverka ytterligare fragmentering av de produktrelaterade cybersäkerhetskraven på den inre marknaden, vilket visas av det breda stödet från olika intressenter för en övergripande åtgärd. Förslaget kommer att minimera den börda för tillverkarna som reglering genom en mångfald av produktsäkerhetslagar innebär. Anpassningen till den nya lagstiftningsramen förbättrar åtgärdens funktionssätt och kontrollen av efterlevnaden. Förslaget rationaliserar processen för skyddsförfaranden genom att involvera tillverkarna och medlemsstaterna innan kommissionen underrättas. En stor andel av de tillverkare som omfattas av förslaget känner redan till hur den nya lagstiftningsramen fungerar, vilket kommer att bidra till förståelsen och genomförandet av förslaget. För konsumenter och företag kommer förslaget att främja förtroendet för produkter med digitala element.

- **Grundläggande rättigheter**

Alla alternativen förväntas i viss mån förbättra skyddet av grundläggande rättigheter och friheter såsom privatliv, skydd av personuppgifter, näringsfrihet och skydd av egendom eller personlig värdighet och integritet. Alternativ 4, som rekommenderas, består av övergripande

regleringsåtgärder och ett brett tillämpningsområde, vilket skulle vara mest ändamålsenligt i detta hänseende, eftersom det är mer sannolikt att det skulle minska antalet incidenter och incidenternas allvarlighetsgrad, inbegripet personuppgiftsincidenter. Det skulle också öka rättssäkerheten och ge lika spelregler för alla ekonomiska aktörer, öka användarnas förtroende och göra EU-produkter med digitala element mer lockande i allmänhet, vilket skyddar egendom och förbättrar villkoren för ekonomiska aktörers kommersiella verksamhet.

De övergripande cybersäkerhetskraven skulle bidra till säkerheten för personuppgifter genom att skydda konfidentialiteten, integriteten och tillgången till information i produkter med digitala element. Uppfyllandet av dessa krav kommer att främja uppfyllandet av de säkerhetskrav för behandling av personuppgifter som fastställs i förordning (EU) 2016/679 (allmän dataskyddsförordning)[12]. Förslaget skulle förbättra transparensen och informationen till användarna, även sådana som inte har så stora cybersäkerhetskunskaper. Användarna skulle också informeras bättre om risker, funktioner och begränsningar hos produkter med digitala element, vilket skulle ge dem bättre möjligheter att vidta de nödvändiga förebyggande och riskreducerande åtgärderna för att minska de kvarstående riskerna.

4. BUDGETKONSEKVENSER

För att fullgöra de uppgifter som tilldelats Europeiska unionens cybersäkerhetsbyrå (Enisa) inom ramen för denna förordning måste Enisa omfördela resurser uppgående till omkring 4,5 heltidsekvivalenter. Kommissionen behöver avsätta 7 heltidsekvivalenter för att kunna fullgöra sina skyldigheter relaterade till kontrollen av efterlevnaden av denna förordning.

En detaljerad översikt över kostnaderna finns i den finansieringsöversikt som åtföljer detta förslag.

5. ÖVRIGA INSLAG

- **Genomförandeplaner samt åtgärder för övervakning, utvärdering och rapportering**

Kommissionen kommer att övervaka genomförandet, tillämpningen och efterlevnaden av dessa nya bestämmelser i syfte att bedöma deras effektivitet. Förordningen kommer att omfatta ett krav på att kommissionen gör en utvärdering och översyn och lämnar en offentlig rapport till Europaparlamentet och rådet senast 36 månader från tillämpningsdatumet och därefter vart fjärde år.

- **Ingående redogörelse för de specifika bestämmelserna i förslaget**

Allmänna bestämmelser (kapitel I)

Den föreslagna förordningen omfattar a) regler för utsläppandet på marknaden av produkter med digitala element, för att säkerställa cybersäkerheten för sådana produkter, b) väsentliga krav för utformningen, utvecklingen och tillverkningen av produkter med digitala element, och skyldigheter för ekonomiska aktörer när det gäller cybersäkerheten för dessa produkter, c) väsentliga krav för de processer för sårbarhetshantering som tillverkarna inför för att säkerställa cybersäkerheten för produkter med digitala element under hela deras livscykel

[12] 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).

samt skyldigheter för ekonomiska aktörer i samband med dessa processer, och d) regler för marknadsövervakning och verkställighet när det gäller ovannämnda regler och krav.

Den föreslagna förordningen kommer att tillämpas på alla produkter med digitala element vars avsedda och rimligen förutsebara användning omfattar en direkt eller indirekt, logisk eller fysisk dataanslutning till en enhet eller ett nät.

Den föreslagna förordningen kommer inte att tillämpas på produkter med digitala element som omfattas av förordning (EU) 2017/745 [medicintekniska produkter för användning på människor och tillbehör till sådana produkter] och förordning (EU) 2017/746 [medicintekniska produkter för in vitro-diagnostik och tillbehör till sådana produkter], eftersom båda dessa förordningar omfattar produktkrav som även omfattar programvara och allmänna skyldigheter för tillverkare, under produkternas hela livscykel, samt förfaranden för bedömning av överensstämmelse. Denna förordning kommer inte att tillämpas på sådana produkter med digitala element som har certifierats i enlighet med förordning 2018/1139 [en hög och enhetlig säkerhetsnivå inom den civila luftfarten] och inte heller på produkter som omfattas av förordning (EU) 2019/2144 [krav för typgodkännande av motorfordon och deras släpvagnar samt de system, komponenter och separata tekniska enheter som är avsedda för sådana fordon].

Kritiska produkter med digitala element ska omfattas av särskilda förfaranden för bedömning av överensstämmelse och ska delas in i klass I och klass II i enlighet med bilaga III, baserat på deras cybersäkerhetsrisknivå, där klass II utgör en större risk. En produkt med digitala element anses kritisk och finns därför med i bilaga III mot bakgrund av effekterna av de potentiella cybersäkerhetssårbarheter som finns i produkten. När cybersäkerhetsrisken fastställs beaktas bland annat de cybersäkerhetsrelaterade funktionerna i en produkt med digitala element och en avsedd användning i känsliga miljöer, såsom en industrimiljö.

Kommissionen ges också befogenhet att anta delegerade akter som kompletterar denna förordning genom att specificera kategorier av mycket kritiska produkter med digitala element för vilka tillverkarna ska vara skyldiga att erhålla ett europeiskt cybersäkerhetscertifikat inom ramen för ett europeiskt system för cybersäkerhetscertifiering, för att visa att de väsentliga krav som anges i bilaga I uppfylls, eller delar av dessa. Vid fastställandet av sådana kategorier av mycket kritiska produkter med digitala element ska kommissionen beakta cybersäkerhetsrisknivån för den berörda kategorin av produkter med digitala element, i ljuset av ett eller flera av de kriterier som beaktas för förteckningen av kritiska produkter med digitala element i bilaga III samt mot bakgrund av bedömningen av om denna produktkategori används av eller krävs för väsentliga entiteter av den typ som avses i bilaga [bilaga I] till direktiv [direktiv XXX/ XXXX (NIS2)] eller kommer att ha en potentiell framtida betydelse för dessa entiteters aktiviteter, eller betydelse för resiliensen mot störande händelser i den totala leveranskedjan för produkter med digitala element.

<u>De ekonomiska aktörernas skyldigheter (kapitel II)</u>

Förslaget omfattar skyldigheter för tillverkarna, importörerna och distributörerna baserat på referensbestämmelserna i beslut 768/2008/EG. De väsentliga cybersäkerhetskraven och skyldigheterna föreskriver för alla produkter med digitala element att de endast får tillhandahållas på marknaden om de tillhandahålls på vederbörligt sätt, är korrekt installerade och underhållna och används för avsett ändamål eller under förhållanden som rimligen kan förutses, och de uppfyller de väsentliga cybersäkerhetskraven enligt denna förordning.

De väsentliga kraven och skyldigheterna skulle innebära att tillverkare måste ta hänsyn till cybersäkerheten vid utformningen, utvecklingen och produktionen av produkter med digitala element, tillämpa tillbörlig aktsamhet i fråga om säkerhetsaspekter vid utformningen och

utvecklingen av sina produkter, vara transparenta i fråga om cybersäkerhetsaspekter som kunderna behöver få kännedom om, säkerställa säkerhetsstöd (uppdateringar) på ett proportionellt sätt och uppfylla kraven i fråga om sårbarhetshantering.

Skyldigheter skulle införas för de ekonomiska aktörerna, från tillverkarna till distributörerna och importörerna, vad gäller utsläppandet på marknaden av produkter med digitala element, på ett sätt som är anpassat till deras roll och ansvar i leveranskedjan.

Överensstämmelse för produkter med digitala element (kapitel III)

En produkt med digitala element som överensstämmer med de harmoniserade standarder eller delar av dem, till vilka hänvisningar har offentliggjorts i *Europeiska unionens officiella tidning*, ska förutsättas överensstämma med de väsentliga kraven i detta förslag till förordning. I de fall då det inte finns några harmoniserade standarder eller dessa är otillräckliga, eller om det standardiseringsförfarandet är förbundet med orimliga förseningar eller kommissionens begäran inte har godtagits av de europeiska standardiseringsorganisationerna, får kommissionen anta gemensamma specifikationer genom genomförandeakter.

Produkter med digitala element som är certifierade eller för vilka en EU-försäkran om överensstämmelse eller ett certifikat har utfärdats inom ett europeiskt system för cybersäkerhetscertifiering i enlighet med förordning (EU) 2019/881, och där kommissionen i en genomförandeakt har specificerat en presumtion om överensstämmelse med denna förordning, ska förutsättas överensstämma med de väsentliga kraven i denna förordning, eller delar därav, i den mån som EU-försäkran om överensstämmelse eller cybersäkerhetscertifikatet, eller delar därav, täcker dessa krav.

För att undvika onödiga administrativa bördor för tillverkarna bör kommissionen, när så är tillämpligt, specificera om ett cybersäkerhetscertifikat som utfärdats inom ett sådant europeiskt system för cybersäkerhetscertifiering eliminerar tillverkarnas skyldighet att genomföra en tredjepartsbedömning av överensstämmelse i enlighet med denna förordning för motsvarande krav.

Tillverkaren ska genomföra en bedömning av överensstämmelse avseende produkten med digitala element och de processer för sårbarhetshantering som den infört för att visa att de väsentliga kraven i bilaga I uppfylls, genom att tillämpa ett av de förfaranden som fastställs i bilaga VI. Tillverkare av kritiska produkter i klass I och II ska använda respektive moduler som krävs för överensstämmelsen. Tillverkare av kritiska produkter i klass II måste involvera tredje part i sin bedömning av överensstämmelse.

Anmälan av organ för bedömning av överensstämmelse (kapitel IV)

För att säkerställa en hög cybersäkerhetsnivå, och för att alla berörda parter ska få förtroende för den ”nya metoden”, är det mycket viktigt att de anmälda organen fungerar korrekt. I enlighet med beslut 768/2008/EG omfattar förslaget därför krav för de nationella myndigheter som ansvarar för organ för bedömning av överensstämmelse (anmälda organ). Enligt förslaget är det i sista hand medlemsstaterna som har ansvaret för att utse och övervaka de anmälda organen. Medlemsstaterna ska utse en anmälande myndighet med ansvar för att inrätta och genomföra de förfaranden som krävs för bedömningen och för anmälan av organ för bedömning av överensstämmelse och övervakningen av anmälda organ.

Marknadskontroll och verkställighet (kapitel V)

I enlighet med förordning (EU) 2019/1020 genomför de nationella marknadskontrollmyndigheterna marknadskontroll på medlemsstatens territorium. Medlemsstaterna får välja att utse en befintlig eller en ny myndighet till att fungera som

marknadskontrollmyndighet, inbegripet nationella behöriga myndigheter enligt artikel [artikel X] i direktiv [direktiv XXX/XXXX (NIS2)] eller utsedda nationella myndigheter för cybersäkerhetscertifiering enligt artikel 58 i förordning (EU) 2019/881. De ekonomiska aktörerna uppmanas att samarbeta fullt ut med marknadskontrollmyndigheterna och andra behöriga myndigheter.

Delegerade befogenheter och kommittéförfarande (kapitel VI)

För att säkerställa att regelverket vid behov kan anpassas bör befogenheten att anta akter i enlighet med artikel 290 i EUF-fördraget delegeras till kommissionen när det gäller uppdatering av förteckningen över kritiska produkter i klass I och II och när det gäller att specificera definitionerna av dessa produktkategorier, specificera om det är nödvändigt med en begränsning eller ett uteslutande av produkter med digitala element som omfattas av andra unionsregler som omfattar krav som ger samma skyddsnivå som denna förordning, införa ett krav på certifiering av vissa mycket kritiska produkter med digitala element baserat på kriterier som fastställs i denna förordning, specificera minimiinnehållet i EU-försäkran om överensstämmelse och komplettera de aspekter som ska ingå i den tekniska dokumentationen.

Kommissionen ges också befogenhet att anta genomförandeakter när det gäller följande: Specificera formatet och vad som ska ingå i rapporteringsskyldigheterna och programvaruförteckningen. Specificera de europeiska system för cybersäkerhetscertifiering som kan användas för att visa överensstämmelse med de väsentliga kraven – eller delar därav – enligt denna förordning. Anta gemensamma specifikationer. Fastställa tekniska specifikationer för anbringande av CE-märkning. Vidta korrigerande eller begränsande åtgärder på unionsnivå under exceptionella omständigheter som motiverar ett omedelbart ingripande för att bevara en välfungerande inre marknad.

Konfidentialitet och sanktioner (kapitel VII)

Alla parter som tillämpar denna förordning ska respektera konfidentialiteten för den information och de data som de erhåller när de utför sina uppgifter och sin verksamhet.

För att säkerställa en effektiv efterlevnadskontroll av de skyldigheter som fastställs i denna förordning bör varje marknadskontrollmyndighet ha befogenhet att påföra eller begära påförande av administrativa sanktionsavgifter. I denna förordning fastställs också maximinivåer för administrativa sanktionsavgifter som bör föreskrivas i nationell lagstiftning vid bristande uppfyllande av skyldigheter enligt denna förordning.

Övergångsbestämmelser och slutbestämmelser (kapitel VIII)

För att ge tillverkare, anmälda organ och medlemsstater tid att anpassa sig till de nya kraven kommer den föreslagna förordningen att bli tillämplig [24 månader] efter ikraftträdandet, med undantag för tillverkarnas rapporteringsskyldighet som börjar gälla [12 månader] efter ikraftträdandet.

2022/0272 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordning (EU) 2019/1020

(Text av betydelse för EES)

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, och

av följande skäl:

(1) Det är nödvändigt att förbättra den inre marknadens funktionssätt genom att fastställa en enhetlig rättslig ram för väsentliga cybersäkerhetskrav för utsläppande av produkter med digitala element på marknaden i unionen. Två stora problem som ökar kostnaderna för användarna och samhället bör lösas: en låg cybersäkerhetsnivå för produkter med digitala element, vilket visas av utbredda sårbarheter och ett otillräckligt och inkonsekvent tillhandahållande av säkerhetsuppdateringar för att åtgärda dessa sårbarheter, samt användarnas bristfälliga förståelse och tillgång till information, vilket hindrar dem från att välja produkter med tillräckliga cybersäkerhetsfunktioner eller att använda dem på ett säkert sätt.

(2) Förordningen syftar till att fastställa randvillkor för utvecklingen av säkra produkter med digitala element genom att säkerställa att hårdvaru- och programvaruprodukter som släpps ut på marknaden har färre sårbarheter och att tillverkarna tar säkerheten på allvar under produktens hela livscykel. Den syftar också till att skapa förutsättningar för att användarna ska kunna ta hänsyn till cybersäkerheten när de väljer och använder produkter med digitala element.

(3) Den relevanta unionslagstiftning som för närvarande gäller omfattar flera uppsättningar övergripande regler som behandlar vissa aspekter av cybersäkerheten från olika synvinklar, inbegripet åtgärder för att förbättra säkerheten i den digitala leveranskedjan. Den befintliga unionslagstiftningen om cybersäkerhet, inbegripet [direktiv XXX/XXXX (NIS2)] och Europaparlamentets och rådets förordning (EU)

[1] EUT C , , s. .
[2] EUT C , , s. .

2019/881[3] täcker inte på ett direkt sätt obligatoriska krav avseende säkerheten för produkter med digitala element.

(4) Den befintliga unionslagstiftningen är visserligen tillämplig på vissa produkter med digitala element, men det finns inget övergripande unionsregelverk med övergripande cybersäkerhetskrav för alla produkter med digitala element. De olika rättsakter och initiativ som hittills har vidtagits på unionsnivå och nationell nivå åtgärdar endast delvis de identifierade cybersäkerhetsrelaterade problemen och riskerna, vilket ger upphov till ett lapptäcke av lagar på den inre marknaden som ökar rättsosäkerheten för både tillverkare och användare av dessa produkter och innebär att det blir onödigt betungande för företagen som måste uppfylla många olika krav för samma typer av produkter. Cybersäkerheten för dessa produkter har en särskilt stark gränsöverskridande dimension, eftersom produkter som tillverkas i ett land ofta används av organisationer och konsumenter på hela den inre marknaden. Därmed är det nödvändigt att reglera detta område på unionsnivå. Unionens regelverk bör harmoniseras genom ett införande av cybersäkerhetskrav för produkter med digitala element. Förutsebarheten bör också säkerställas för aktörer och användare i hela unionen och harmoniseringen förbättras på den inre marknaden, vilket skapar hållbarare villkor för operatörer som vill komma in på unionsmarknaden.

(5) På unionsnivå har särskilda EU-cybersäkerhetskrav efterlysts för digitala eller uppkopplade produkter, exempelvis i EU:s cybersäkerhetsstrategi för det digitala decenniet[4], rådets slutsatser av den 2 december 2020 och den 23 maj 2022 och Europaparlamentets resolution av den 10 juni 2021[5], och flera länder runtom i världen håller på att vidta åtgärder för att åtgärda detta på eget initiativ. I slutrapporten från konferensen om Europas framtid[6] efterlyste medborgarna ”En starkare roll för EU när det gäller att motverka cybersäkerhetshot”.

(6) För att höja den allmänna cybersäkerhetsnivån för alla produkter med digitala element som släpps ut på den inre marknaden är det nödvändigt att införa målinriktade och teknikneutrala väsentliga cybersäkerhetskrav för dessa produkter vilka ska tillämpas horisontellt.

(7) Under vissa omständigheter kan alla produkter med digitala element vilka är integrerade i eller anslutna till ett större elektroniskt informationssystem fungera som en attackvektor för fientliga aktörer. Det innebär att även hårdvara eller programvara som anses mindre kritisk kan underlätta en inledande kompromettering av en enhet eller ett nät, vilket gör det möjligt för fientliga aktörer att få priviligierad åtkomst till ett system eller röra sig lateralt mellan system. Tillverkarna bör därför säkerställa att alla uppkopplingsbara produkter med digitala element utformas och utvecklas i enlighet med de väsentliga krav som fastställs i denna förordning. Detta innefattar både produkter som kan anslutas fysiskt via hårdvarugränssnitt och produkter som

---

[3] 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).

[4] JOIN(2020) 18 final, https://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:52020JC0018&from=EN.

[5] 2021/2568(RSP), https://www.europarl.europa.eu/doceo/document/TA-9-2021-0286_SV.html.

[6] *Konferensen om Europas framtid – Rapport om det slutliga resultatet*, maj 2022, förslag 28 (åtgärd 2). Konferensen hölls mellan april 2021 och maj 2022. Det var en unik medborgarledd samtalsdemokrati på alleuropeisk nivå, med deltagande av tusentals EU-medborgare samt politiska aktörer, arbetsmarknadens parter, företrädare för det civila samhället och viktiga intressenter.

ansluts logiskt, t.ex. via nätanslutningsuttag, rör, filer, programmeringsgränssnitt eller andra typer av programvarugränssnitt. I och med att cybersäkerhetshot kan spridas via olika produkter med digitala element tills de når ett visst mål, exempelvis genom att sammanlänka flera olika attacker mot sårbarheter, bör tillverkarna också säkerställa cybersäkerheten för produkter som endast indirekt ansluts till andra enheter eller nät.

(8) Genom att cybersäkerhetskrav fastställs för utsläppandet på marknaden av produkter med digitala element kommer dessa produkters cybersäkerhet att förbättras för både konsumenter och företag. Detta innefattar krav för utsläppandet på marknaden av konsumentprodukter med digitala element vilka är avsedda för sårbara konsumenter, exempelvis leksaker och babyvakter.

(9) Denna förordning säkerställer en hög cybersäkerhetsnivå för produkter med digitala element. Den reglerar inte tjänster, såsom program som nättjänst (SaaS), förutom när det gäller lösningar för fjärrbehandling av data relaterade till en produkt med digitala element vilket ska förstås som all databehandling på distans för vilken programvaran har utformats och utvecklats av den berörda produktens tillverkare eller under dennes ansvar, och vars avsaknad skulle innebära att en sådan produkt med digitala element inte skulle kunna utföra en av sina funktioner. Genom [direktiv XXX/XXXX (NIS2)] införs krav på cybersäkerhet och rapportering av incidenter för väsentliga och viktiga entiteter, såsom kritisk infrastruktur, i syfte att stärka resiliensen för de tjänster dessa tillhandahåller. [Direktiv XXX/XXXX (NIS2)] är tillämpligt på datormoln och molntjänstmodeller, såsom SaaS. Alla enheter som tillhandahåller molntjänster i unionen och som uppnår eller överskrider tröskeln för medelstora företag omfattas av det direktivet.

(10) För att inte stå i vägen för innovation eller forskning bör fri programvara med öppen källkod som utvecklas eller tillhandahålls utanför ramen för kommersiell verksamhet inte omfattas av denna förordning. Detta gäller i synnerhet för programvara, inbegripet källkod och modifierade versioner, som delas öppet och är fritt tillgänglig, användbar och modifierbar och som kan vidaredistribueras. När det gäller programvara kan en kommersiell verksamhet inte bara kännetecknas av att det tas ut en avgift för produkten utan också av att en avgift tas ut för tekniska stödtjänster, att en programvaruplattform tillhandahålls som tillverkaren använder för att monetarisera andra tjänster eller av att personuppgifter används för andra syften än uteslutande att förbättra programvarans säkerhet, kompatibilitet eller interoperabilitet.

(11) Ett säkert internet är avgörande för att kritiska infrastrukturer och samhället som helhet ska kunna fungera. [Direktiv XXX/XXXX (NIS2)] syftar till att säkerställa en hög cybersäkerhetsnivå för tjänster som tillhandahålls av väsentliga och viktiga entiteter, inbegripet leverantörer av digital infrastruktur som stöder kärnfunktioner för ett öppet internet eller säkerställer internetåtkomst och internettjänster. Det är därför viktigt att de produkter med digitala element som behövs för att leverantörer av digital infrastruktur ska kunna säkerställa ett fungerande internet utvecklas på ett säkert sätt och att de uppfyller väletablerade internetsäkerhetsstandarder. Denna förordning, som är tillämplig på alla uppkopplingsbara hårdvaru- och programvaruprodukter, syftar också till att främja att leverantörer av digital infrastruktur uppfyller leveranskedjekraven enligt [direktiv XXX/XXXX (NIS2)] genom att säkerställa att de produkter med digitala element som de använder för tillhandahållandet av sina tjänster utvecklas på ett säkert sätt och att de har tillgång till säkerhetsuppdateringar i rätt tid för sådana produkter.

(12) I Europaparlamentets och rådets förordning (EU) 2017/745[7] fastställs bestämmelser om medicintekniska produkter och i Europaparlamentets och rådets förordning (EU) 2017/746[8] fastställs bestämmelser om medicintekniska produkter för in vitro-diagnostik. Båda förordningarna behandlar cybersäkerhetsrisker enligt särskilda tillvägagångssätt som också behandlas i denna förordning. Närmare bestämt fastställs i förordningarna (EU) 2017/745 och (EU) 2017/746 väsentliga krav för medicintekniska produkter som fungerar genom ett elektroniskt system eller som själva utgörs av programvara. Viss icke-inbyggd programvara och ett livscykelperspektiv täcks också av dessa förordningar. Dessa krav innebär att tillverkarna ska utveckla och bygga sina produkter genom att tillämpa riskhanteringsprinciper och genom att fastställa krav på it-säkerhetsåtgärder, samt motsvarande förfaranden för bedömning av överensstämmelse. Vidare finns det sedan december 2019 särskilda riktlinjer för cybersäkerheten för medicintekniska produkter, som ger tillverkarna av medicintekniska produkter, däribland för in vitro-diagnostik, vägledning för hur alla berörda väsentliga krav i bilaga I till dessa förordningar ska uppfyllas när det gäller cybersäkerhet[9]. Produkter med digitala element på vilka någon av dessa förordningar är tillämpliga bör därför inte omfattas av denna förordning.

(13) Genom Europaparlamentets och rådets förordning (EU) 2019/2144[10] fastställs krav för typgodkännande av fordon och deras system och komponenter, som innebär att vissa cybersäkerhetskrav införs, inbegripet när det gäller användning av ett certifierat ledningssystem för cybersäkerhet och uppdateringar av programvara, som täcker organisationers policyer och processer för cyberrisker under hela livscykeln för fordon, utrustning och tjänster i enlighet med tillämpliga FN-föreskrifter om tekniska specifikationer och cybersäkerhet[11], och föreskrivs särskilda förfaranden för bedömning av överensstämmelse. På luftfartsområdet är huvudsyftet för Europaparlamentets och rådets förordning (EU) 2018/1139[12] att fastställa och upprätthålla en hög och enhetlig säkerhetsnivå inom den civila luftfarten i unionen. Förordningen ger en ram för väsentliga krav på luftvärdighet för luftfartsprodukter, delar och utrustning, inbegripet programvara som beaktar skyldigheten att skydda sig mot informationssäkerhetshot. Produkter med digitala element som omfattas av förordning (EU) 2019/2144 och produkter som certifierats i enlighet med förordning (EU) 2018/1139 omfattas därför inte av de väsentliga krav och förfaranden för bedömning av överensstämmelse som fastställs i denna förordning.

---

7 Europaparlamentets och rådets förordning (EU) 2017/745 av den 5 april 2017 om medicintekniska produkter, om ändring av direktiv 2001/83/EG, förordning (EG) nr 178/2002 och förordning (EG) nr 1223/2009 och om upphävande av rådets direktiv 90/385/EEG och 93/42/EEG (EUT L 117, 5.5.2017, s. 1).

8 Europaparlamentets och rådets förordning (EU) 2017/746 av den 5 april 2017 om medicintekniska produkter för in vitro-diagnostik och om upphävande av direktiv 98/79/EG och kommissionens beslut 2010/227/EU (EUT L 117, 5.5.2017, s. 176).

9 MDCG 2019-16, som godkänts av samordningsgruppen för medicintekniska produkter som inrättades genom artikel 103 i förordning (EU) 2017/745.

10

11 FN-föreskrift nr 155 – Enhetliga bestämmelser om godkännande av fordon med avseende på cybersäkerhet och ledningssystem för cybersäkerhet [2021/387].

12 Europaparlamentets och rådets förordning (EU) 2018/1139 av den 4 juli 2018 om fastställande av gemensamma bestämmelser på det civila luftfartsområdet och inrättande av Europeiska unionens byrå för luftfartssäkerhet, och om ändring av Europaparlamentets och rådets förordningar (EG) nr 2111/2005, (EG) nr 1008/2008, (EU) nr 996/2010, (EU) nr 376/2014 och direktiv 2014/30/EU och 2014/53/EU, samt om upphävande av Europaparlamentets och rådets förordningar (EG) nr 552/2004 och (EG) nr 216/2008 och rådets förordning (EEG) nr 3922/91 (EUT L 212, 22.8.2018, s. 1).

Certifieringsförfarandena enligt förordning (EU) 2018/1139 säkerställer den assuransnivå som eftersträvas i denna förordning.

(14) Genom denna förordning fastställs övergripande cybersäkerhetsregler som inte är sektorsspecifika eller specifika för vissa produkter med digitala element. Sektors- eller produktspecifika unionsregler kan dock införas, med krav som omfattar alla eller vissa risker som täcks av de väsentliga kraven enligt denna förordning. I sådana fall får tillämpningen av denna förordning på sådana produkter med digitala element som omfattas av andra unionsregler, där krav fastställs avseende alla eller vissa risker som täcks av de väsentliga kraven i bilaga I till denna förordning, begränsas eller uteslutas när en begränsning eller ett uteslutande är förenligt med den allmänna rättsliga ram som är tillämplig på dessa produkter och när sektorsreglerna ger samma skyddsnivå som denna förordning. Kommissionen bör ges befogenhet att anta delegerade akter för att ändra denna förordning genom att identifiera sådana produkter och regler. För befintlig unionslagstiftning på vilken denna typ av begränsning eller uteslutande bör tillämpas, omfattar denna förordning särskilda bestämmelser som klargör dess förhållande till den unionslagstiftningen.

(15) I delegerad förordning (EU) 2022/30 specificeras att de väsentliga krav som fastställs i artikel 3.3 d (skada på nät och felaktig användning av nätresurser), e (personuppgifter och personlig integritet) och f (bedrägeri) i direktiv 2014/53/EU ska tillämpas på viss radioutrustning. I [kommissionens genomförandebeslut XXX/2022 om en standardiseringsbegäran till de europeiska standardiseringsorganisationerna] fastställs krav för utarbetandet av särskilda standarder som ytterligare specificerar hur dessa tre väsentliga krav bör hanteras. De väsentliga krav som fastställs i denna förordning omfattar alla aspekter av de väsentliga krav som avses i artikel 3.3 d, e och f i direktiv 2014/53/EU. De väsentliga kraven i denna förordning är också anpassade till syftena för kraven på särskilda standarder som omfattas av den standardiseringsbegäran. Om kommissionen upphäver eller ändrar delegerad förordning (EU) 2022/30 med följden att den upphör att gälla för vissa produkter som omfattas av denna förordning, bör kommissionen och de europeiska standardiseringsorganisationerna, i samband med förberedelserna och utarbetandet av harmoniserade standarder för att underlätta genomförandet av denna förordning, ta hänsyn till det standardiseringsarbete som utförts inom ramen för kommissionens genomförandebeslut C(2022)5637 om en begäran om standardisering för delegerad förordning 2022/30.

(16) Direktiv 85/374/EEG[13] kompletterar denna förordning. Genom det direktivet fastställs skadeståndsansvar för produkter med säkerhetsbrister så att skadelidande kan kräva ersättning när en skada har orsakats av produkter med säkerhetsbrister. Där fastställs principen att tillverkaren av en produkt har skadeståndsansvaret för skador som orsakats av säkerhetsbrister i produkten oavsett om tillverkaren agerat oaktsamt (*strikt ansvar*) När sådana säkerhetsbrister består av en brist på säkerhetsuppdateringar efter att produkten släppts ut på marknaden och detta orsakar skada kan tillverkarens skadeståndsansvar utlösas. Tillverkarnas skyldigheter avseende tillhandahållandet av sådana säkerhetsuppdateringar bör fastställas i denna förordning.

[13] Rådets direktiv 85/374/EEG av den 25 juli 1985 om tillnärmning av medlemsstaternas lagar och andra författningar om skadeståndsansvar för produkter med säkerhetsbrister (EGT L 210, 7.8.1985).

(17) Denna förordning bör inte påverka tillämpningen av Europaparlamentets och rådets förordning (EU) 2016/679[14], inklusive när det gäller bestämmelser om inrättandet av certifieringsmekanismer för dataskydd och sigill och märkningar för dataskydd som syftar till att visa att personuppgiftsansvarigas och personuppgiftsbiträdens databehandling uppfyller kraven i den förordningen. Sådan behandling kan vara inbyggd i en produkt med digitala element. Inbyggt dataskydd och dataskydd som standard samt allmän cybersäkerhet är viktiga aspekter av förordning (EU) 2016/679. Genom att skydda konsumenter och organisationer från cybersäkerhetsrisker bidrar de väsentliga cybersäkerhetskrav som fastställs i denna förordning till att förbättra skyddet av personuppgifter och individers personliga 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 (EDPB), som inrättats genom förordning (EU) 2016/679, och de nationella tillsynsmyndigheterna med ansvar för dataskydd. Synergier mellan denna förordning och unionens dataskyddslagstiftning bör också skapas på områdena marknadskontroll och kontroll av efterlevnaden. Därför bör de nationella marknadskontrollmyndigheter som utses enligt denna förordning samarbeta med de myndigheter som utövar tillsyn över unionens dataskyddslagstiftning. De sistnämnda bör också ha tillgång till information av relevans för utförandet av deras uppgifter.

(18) I den mån som deras produkter omfattas av den här förordningen bör utfärdare av europeiska e-identitetsplånböcker enligt artikel [artikel 6a.2 i förordning (EU) nr 910/2014, ändrad genom förslag till förordning om ändring av förordning (EU) nr 910/2014 vad gäller inrättandet av en ram för europeisk digital identitet] uppfylla både de övergripande väsentliga krav som fastställs i den här förordningen och de särskilda säkerhetskrav som fastställs i artikel [artikel 6a i förordning (EU) nr 910/2014, ändrad genom förslag till förordning om ändring av förordning (EU) nr 910/2014 vad gäller inrättandet av en ram för europeisk digital identitet]. För att främja efterlevnad bör utfärdarna kunna visa att europeiska e-identitetsplånböcker uppfyller de krav som fastställs i båda dessa rättsakter genom att låta certifiera sina produkter inom ett europeiskt system för cybersäkerhetscertifiering som inrättas inom ramen för förordning (EU) 2019/881 och för vilket kommissionen genom en genomförandeakt specificerat en presumtion om överensstämmelse för denna förordning, i den mån som certifikatet, eller delar av detta, täcker dessa krav.

(19) Vissa uppgifter som föreskrivs i denna förordning bör utföras av Enisa, i enlighet med artikel 3.2 i förordning (EU) 2019/881. Enisa bör i synnerhet ta emot anmälningar från tillverkare om aktivt utnyttjade sårbarheter i produkter med digitala element samt om incidenter som påverkar säkerheten för dessa produkter. Enisa bör också vidarebefordra dessa anmälningar till de berörda CSIRT-enheterna eller medlemsstaternas berörda gemensamma kontaktpunkter som utsetts i enlighet med artikel [artikel X] i direktiv [direktiv XXX / XXXX (NIS2)] samt underrätta berörda marknadskontrollmyndigheter om de anmälda sårbarheterna. På grundval av sin insamlade information bör Enisa vartannat år utarbeta en teknisk rapport om nya trender i fråga om cybersäkerhetsrisker i produkter med digitala element, och lämna

[14] 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).

den till den samarbetsgrupp som avses i direktiv [direktiv XXX / XXXX (NIS2)]. Med tanke på Enisas sakkunskaper och uppdrag bör Enisa också kunna stödja processen för genomförande av denna förordning. Enisa bör i synnerhet kunna föreslå gemensamma åtgärder som ska vidtas av marknadskontrollmyndigheter i flera medlemsstater på grundval av indikationer eller information om potentiell bristande överensstämmelse med denna förordning för produkter med digitala element eller identifiera produktkategorier där samtidiga samordnade kontrollåtgärder bör organiseras. Under exceptionella omständigheter bör Enisa, på kommissionens begäran, kunna göra utvärderingar av specifika produkter med digitala element som utgör en betydande cybersäkerhetsrisk, när ett omedelbart ingripande krävs för att bevara en välfungerande inre marknad.

(20) Produkter med digitala element bör vara försedda med en CE-märkning som visar att de överensstämmer med denna förordning, så att de omfattas av den fria rörligheten på den inre marknaden. Medlemsstaterna bör inte sätta upp omotiverade hinder för utsläppandet på marknaden av produkter med digitala element som uppfyller kraven i denna förordning och är försedda med en CE-märkning.

(21) För att säkerställa att tillverkarna kan släppa ut programvara i testsyfte innan deras produkter genomgår en bedömning av överensstämmelse bör medlemsstaterna inte hindra tillhandahållandet av ofärdig programvara, såsom alfaversioner, betaversioner eller lanseringskandidater, så länge som versionen endast görs tillgänglig så lång tid som de behöver för att testa den och få återkoppling. Tillverkarna bör säkerställa att programvara som görs tillgänglig under dessa villkor inte släpps ut förrän en riskbedömning har gjorts och att den i möjligaste mån uppfyller de säkerhetskrav som enligt denna förordning gäller för egenskaper hos produkter med digitala element. Tillverkarna bör också i möjligaste mån uppfylla sårbarhetshanteringskraven. Tillverkarna bör inte tvinga användare att uppgradera till versioner som endast släppts ut i testsyfte.

(22) För att säkerställa att produkter med digitala element inte utgör cybersäkerhetsrisker för personer och organisationer när de släpps ut på marknaden bör väsentliga krav fastställas för sådana produkter. När produkterna senare, fysiskt eller digitalt, ändras på ett sätt som tillverkaren inte förutsett och som kan innebära att de inte längre uppfyller de relevanta väsentliga kraven, bör ändringen betraktas som väsentlig. Exempelvis kan programvaruuppdateringar eller programvarureparationer betraktas som underhållsåtgärder, förutsatt att de inte ändrar en produkt som redan släppts ut på marknaden på ett sådant sätt att överensstämmelsen med de tillämpliga kraven kan påverkas eller att den avsedda användning för vilken produkten har bedömts kan ändras. Precis som när det gäller fysiska reparationer eller ändringar bör en produkt med digitala element anses ha ändrats väsentligt genom en programvaruändring om uppdateringen av programvaran ändrar produktens ursprungliga avsedda funktioner eller produktens typ eller prestanda, och dessa ändringar inte förutsågs i den ursprungliga riskbedömningen, eller om arten av hot har ändrats eller risknivån har höjts på grund av uppdateringen.

(23) I linje med det vedertagna begreppet väsentlig ändring för produkter som regleras genom unionens harmoniseringslagstiftning, är det, vid en väsentlig ändring som kan påverka produktens överensstämmelse med denna förordning eller om produktens avsedda ändamål ändras, lämpligt att produktens överensstämmelse kontrolleras och att den, om tillämpligt, genomgår en ny bedömning av överensstämmelse. Om tillverkaren låter göra en bedömning av överensstämmelse som involverar tredje part

bör förändringar som kan leda till väsentliga ändringar i tillämpliga fall anmälas till denna tredje part.

(24) Renovering, underhåll och reparation av en produkt med digitala element, enligt definitionen i förordning [förordningen om ekodesign], medför inte nödvändigtvis en väsentlig ändring av produkten, exempelvis om den avsedda användningen och funktionerna inte ändras och risknivån inte påverkas. Tillverkarens uppgradering av en produkt kan dock medföra ändringar av produktens utformning och utveckling och kan därför påverka produktens avsedda användning och uppfyllande av de krav som fastställs i denna förordning.

(25) Produkter med digitala element bör anses som kritiska om de negativa konsekvenserna av utnyttjandet av potentiella cybersäkerhetssårbarheter i produkten kan vara allvarliga på grund av, bland annat, cybersäkerhetsrelaterade funktioner eller produktens avsedda användning. Sårbarheter i produkter med digitala element som har en cybersäkerhetsrelaterad funktion, såsom säkra element, kan medföra att säkerhetsproblem sprids i hela leveranskedjan. Allvarlighetsgraden i en cybersäkerhetsincident kan också öka när produktens avsedda användning beaktas, t.ex. om det handlar om en industriell miljö eller en väsentlig entitet av den typ som avses i bilaga [bilaga I] till direktiv [direktiv XXX/ XXXX (NIS2)] eller användning för utförandet av kritiska eller känsliga funktioner, såsom behandling av personuppgifter.

(26) Kritiska produkter med digitala element bör omfattas av striktare förfaranden för bedömning av överensstämmelse, med bevarande av proportionaliteten. Därför bör kritiska produkter med digitala element delas in i två klasser som återspeglar produktkategoriernas cybersäkerhetsrisknivå. En potentiell cyberincident som involverar produkter i klass II kan få större negativa konsekvenser än en incident som involverar produkter i klass I, exempelvis på grund av produkternas cybersäkerhetsrelaterade funktion eller avsedda användning i känsliga miljöer; de bör därför omfattas av ett striktare förfarande för bedömning av överensstämmelse.

(27) De kategorier av kritiska produkter med digitala element som avses i bilaga III till denna förordning bör förstås som produkter vars kärnfunktioner är av en typ som förtecknas i bilaga III till denna förordning. I bilaga III till denna förordning förtecknas exempelvis produkter som genom sina kärnfunktioner definieras som generella mikroprocessorer i klass II. Därmed bör mikroprocessorer för allmänna ändamål genomgå en obligatorisk tredjepartsbedömning av överensstämmelse. Detta är inte fallet för andra produkter som inte uttryckligen nämns i bilaga III till denna förordning men som kan innehålla en generell mikroprocessor. Kommissionen bör anta delegerade akter [senast 12 månader efter denna förordnings ikraftträdande] för att specificera definitionerna av de produktkategorier som omfattas av klass I respektive klass II enligt bilaga III.

(28) Denna förordning behandlar cybersäkerhetsrisker på ett målinriktat sätt. Produkter med digitala element kan dock utgöra andra säkerhetsrisker än sådana som rör cybersäkerheten. Dessa risker bör även fortsättningsvis regleras av annan relevant produktlagstiftning på unionsnivå. Om ingen annan del av unionens harmoniseringslagstiftning är tillämplig bör de omfattas av förordning [förordningen om allmän produktsäkerhet]. Mot bakgrund av denna förordnings fokus och som en avvikelse från artikel 2.1 tredje stycket b i förordning [förordningen om allmän produktsäkerhet], bör kapitel III avsnitt 1, kapitel V och VII och kapitel IX–XI i förordning [förordningen om allmän produktsäkerhet] tillämpas på produkter med

digitala element med avseende på säkerhetsrisker som inte omfattas av denna förordning, om produkterna inte omfattas av särskilda krav enligt andra bestämmelser i unionens harmoniseringslagstiftning i den mening som avses i [artikel 3.25 i förordningen om allmän produktsäkerhet].

(29) Produkter med digitala element som klassificeras som AI-system med hög risk enligt definitionen i artikel 6 i förordning[15] [AI-förordningen] och som omfattas av denna förordning bör uppfylla de väsentliga krav som fastställs i denna förordning. När sådana AI-system med hög risk uppfyller de väsentliga kraven i denna förordning bör de anses uppfylla de cybersäkerhetskrav som fastställs i artikel [artikel 15] i förordning [AI-förordningen] i den mån som dessa krav omfattas av en EU-försäkran om överensstämmelse som utfärdats i enlighet med denna förordning, eller delar av denna. När det gäller de förfaranden för bedömning av överensstämmelse avseende väsentliga cybersäkerhetskrav för en produkt med digitala element som omfattas av denna förordning och klassificeras som ett AI-system med hög risk, bör de relevanta bestämmelserna i artikel 43 i förordning [AI-förordningen] tillämpas som regel i stället för respektive bestämmelser i denna förordning. Denna regel bör dock inte leda till att den nödvändiga assuransnivån sänks för kritiska produkter med digitala element som omfattas av denna förordning. Med avvikelse från denna regel bör därför också AI-system med hög risk som omfattas av förordning [AI-förordningen] och som också kategoriseras som kritiska produkter med digitala element enligt denna förordning, och på vilka förfarandet för bedömning av överensstämmelse baserat på intern kontroll enligt bilaga VI i förordning [AI-förordningen] är tillämpligt, omfattas av denna förordnings bestämmelser om bedömning av överensstämmelse i den mån som de väsentliga kraven i denna förordning berörs. När det gäller alla andra aspekter som omfattas av förordning [AI-förordningen], bör i sådana fall respektive bestämmelser om bedömning av överensstämmelse baserad på intern kontroll vilka fastställs i bilaga VI till förordning [AI-förordningen] tillämpas.

(30) Maskinprodukter som omfattas av förordning [förordningen om maskinprodukter] och som är produkter med digitala element i den mening som avses i denna förordning, och för vilka en försäkran om överensstämmelse har utfärdats på grundval av denna förordning, bör anses uppfylla de väsentliga hälso- och säkerhetskrav som fastställs i [avsnitt 1.1.9 och 1.2.1 i bilaga III] till förordning [förordningen om maskinprodukter], vad gäller skydd mot förvanskning samt säkerhet och tillförlitlighet i kontrollsystemen, i den mån som överensstämmelsen med dessa krav styrks genom en EU-försäkran om överensstämmelse som utfärdats i enlighet med denna förordning.

(31) Förordning [förslag till förordning om ett europeiskt hälsodataområde] kompletterar de väsentliga krav som fastställs i denna förordning. Elektroniska patientjournalsystem som omfattas av förordning [förslag till förordning om ett europeiskt hälsodataområde] och som är produkter med digitala element i den mening som avses i denna förordning, bör därför också uppfylla de väsentliga krav som fastställs i denna förordning. Tillverkarna bör visa överensstämmelse i enlighet med förordning [förslag till förordning om ett europeiskt hälsodataområde]. För att främja efterlevnaden får tillverkarna upprätta en enda teknisk dokumentation som täcker alla aspekter som krävs enligt båda rättsakterna. I och med att denna förordning inte täcker SaaS som sådant omfattas elektroniska patientjournalsystem som erbjuds genom SaaS-licens- och leveransmodellen inte av denna förordning. Elektroniska patientjournalsystem

[15] Förordning [AI-förordningen].

som utvecklas och används internt omfattas inte heller av denna förordning eftersom de inte släpps ut på marknaden.

(32) För att säkerställa att produkter med digitala element är säkra både när de släpps ut på marknaden och under hela sin livscykel, är det nödvändigt att fastställa väsentliga krav för sårbarhetshantering och väsentliga cybersäkerhetskrav för egenskaperna hos produkter med digitala element. Tillverkarna bör uppfylla alla väsentliga krav som rör sårbarhetshantering och säkerställa att alla deras produkter levereras utan några kända sårbarheter som kan utnyttjas och de bör fastställa vilka andra väsentliga krav på produktegenskaper som är relevanta för den berörda produkttypen. Därför bör tillverkarna göra en bedömning av vilka cybersäkerhetsrisker som är förbundna med en produkt med digitala element, för att identifiera relevanta risker och relevanta väsentliga krav och tillämpa lämpliga harmoniserade standarder eller gemensamma specifikationer.

(33) För att förbättra säkerheten för produkter med digitala element som släpps ut på den inre marknaden är det nödvändigt att fastställa väsentliga krav. Dessa väsentliga krav bör inte påverka tillämpningen av EU-samordnade riskbedömningar av kritiska leveranskedjor enligt [artikel X] i direktiv [direktiv XXX/XXXX(NIS2)][16], som beaktar både tekniska och, när så är relevant, icke-tekniska riskfaktorer, såsom tredjelands otillbörliga påverkan på leverantörer. Det bör inte heller påverka medlemsstaternas rätt att fastställa ytterligare krav för att ta hänsyn till icke-tekniska faktorer för att säkerställa en hög resiliensnivå, inbegripet krav som definieras i rekommendation (EU) 2019/534, den unionssamordnade riskbedömningen av säkerhet i 5G-nät och EU-verktygslådan för 5G-cybersäkerhet som överenskommits av samarbetsgruppen för nät- och informationssäkerhet enligt [direktiv XXX/XXXX (NIS2)].

(34) För att säkerställa att de nationella CSIRT-enheterna och de gemensamma kontaktpunkter som utses i enlighet med artikel [artikel X] i direktiv [direktiv XX/XXXX (NIS2)] förses med den information som de behöver för att utföra sina uppgifter och höja den allmänna cybersäkerhetsnivån för väsentliga och viktiga entiteter, och för att säkerställa att marknadskontrollmyndigheterna fungerar effektivt, bör tillverkare av produkter med digitala element anmäla aktivt utnyttjade sårbarheter till Enisa. I och med att de flesta produkter med digitala element saluförs på hela den inre marknaden bör varje utnyttjad sårbarhet i en produkt med digitala element anses som ett hot mot en fungerande inre marknad. Tillverkarna bör också överväga att meddela åtgärdade sårbarheter till den europeiska sårbarhetsdatabas som inrättats enligt direktiv [direktiv XX/XXXX (NIS2)] och förvaltas av Enisa eller till någon annan allmänt tillgänglig sårbarhetsdatabas.

(35) Tillverkarna bör också rapportera alla incidenter som påverkar säkerheten för produkter med digitala element till Enisa. Utan hinder av incidentrapporteringsskyldigheterna enligt direktiv [direktiv XXX/XXXX (NIS2)] för väsentliga och viktiga entiteter är det mycket viktigt att Enisa, de gemensamma kontaktpunkter som utsetts av medlemsstaterna i enlighet med artikel [artikel X] i direktiv [direktiv XXX/XXXX (NIS2)] och marknadskontrollmyndigheterna får information från tillverkare av produkter med digitala element så att de kan bedöma

[16] Europaparlamentets och rådets direktiv XXX av den [datum] [om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, och om upphävande av direktiv (EU) 2016/1148 (EUT L xx, datum, s. x)].

säkerheten för dessa produkter. För att säkerställa att användarna kan reagera snabbt på incidenter som påverkar säkerheten för deras produkter med digitala element, bör tillverkarna också underrätta sina användare om alla sådana incidenter och, om tillämpligt, om eventuella korrigerande åtgärder som användarna kan vidta för att begränsa konsekvenserna av incidenten, exempelvis genom att offentliggöra relevant information på sina webbplatser eller, om tillverkaren kan kontakta användarna och det är motiverat med tanke på riskerna, genom att vända sig direkt till användarna.

(36) Tillverkare av produkter med digitala element bör införa samordnade policyer för information om sårbarheter för att underlätta individers eller entiteters rapportering av sårbarheter. En samordnad policy för offentliggörande av sårbarheter bör specificera en strukturerad process där sårbarheter rapporteras till en tillverkare på ett sådant sätt att tillverkaren kan diagnostisera och åtgärda dessa sårbarheter innan mer detaljerad sårbarhetsinformation lämnas ut till tredje part eller till allmänheten. I och med att information om sårbarheter som kan utnyttjas hos allmänt använda produkter med digitala element kan säljas till höga priser på den svarta marknaden bör tillverkare av sådana produkter som ett led i sina samordnade policyer för information om sårbarheter kunna använda program för att ge incitament till rapportering av sårbarheter genom att säkerställa att individer eller entiteter får erkännande och ersättning för sina insatser (så kallade *buggbelöningsprogram*).

(37) För att underlätta sårbarhetsanalys bör tillverkarna identifiera och dokumentera de komponenter som ingår i produkter med digitala element, exempelvis genom att utarbeta en programvaruförteckning. En programvaruförteckning kan förse dem som tillverkar, köper och driver programvara med information som förbättrar deras förståelse av leveranskedjan, vilket har många fördelar, framför allt att det hjälper tillverkare och användare att spåra kända nya sårbarheter och risker. Det är särskilt viktigt för tillverkarna att säkerställa att deras produkter inte innehåller sårbara komponenter som utvecklats av tredje part.

(38) För att underlätta bedömningen av överensstämmelse med de krav som fastställs i denna förordning bör det finnas en presumtion om överensstämmelse för produkter med digitala element som överensstämmer med harmoniserade standarder som omsätter de väsentliga kraven i denna förordning till detaljerade tekniska specifikationer och som antas i enlighet med Europaparlamentets och rådets förordning (EU) nr 1025/2012[17]. I förordning (EU) nr 1025/2012 fastställs ett förfarande för invändningar mot harmoniserade standarder som inte helt uppfyller kraven i denna förordning.

(39) Genom förordning (EU) 2019/881 inrättas en frivillig europeisk ram för cybersäkerhetscertifiering av IKT-produkter, -processer och -tjänster. De europeiska systemen för cybersäkerhetscertifiering kan omfatta produkter med digitala element vilka omfattas av denna förordning. Denna förordning bör skapa synergier med förordning (EU) 2019/881. För att främja bedömningen av överensstämmelse med kraven i denna förordning, när det gäller produkter med digitala element som är certifierade eller för vilka en försäkran om överensstämmelse har utfärdats inom ett cybersäkerhetssystem i enlighet med förordning (EU) 2019/881 och som har

[17] Europaparlamentets och rådets förordning (EU) nr 1025/2012 av den 25 oktober 2012 om europeisk standardisering och om ändring av rådets direktiv 89/686/EEG och 93/15/EEG samt av Europaparlamentets och rådets direktiv 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG och 2009/105/EG samt om upphävande av rådets beslut 87/95/EEG och Europaparlamentets och rådets beslut nr 1673/2006/EG (EUT L 316, 14.11.2012, s. 12).

identifierats av kommissionen i en genomförandeakt, bör det finnas en presumtion om överensstämmelse med de väsentliga kraven i denna förordning i den mån som cybersäkerhetscertifikatet eller försäkran om överensstämmelse – eller delar av dessa – täcker dessa krav. Behovet av nya europeiska system för cybersäkerhetscertifiering av produkter med digitala element bör bedömas i ljuset av denna förordning. Sådana framtida europeiska cybersäkerhetscertifieringssystem som omfattar produkter med digitala element bör beakta de väsentliga krav som fastställs i denna förordning och främja efterlevnaden av denna förordning. Kommissionen bör ha befogenhet att genom genomförandeakter specificera de europeiska system för cybersäkerhetscertifiering som kan användas för att visa överensstämmelse med de väsentliga krav som fastställs i denna förordning. För att undvika onödiga administrativa bördor för tillverkarna bör kommissionen, när så är tillämpligt, specificera om ett cybersäkerhetscertifikat som utfärdats inom sådana europeiska system för cybersäkerhetscertifiering befriar tillverkarna från skyldigheten att genomföra en tredjepartsbedömning av överensstämmelse i enlighet med denna förordning för motsvarande krav.

(40) Vid ikraftträdandet av en genomförandeakt [kommissionens genomförandeförordning (EU) nr …/... av den XXX om ett europeiskt system för cybersäkerhetscertifiering baserat på gemensamma kriterier (EUCC)] som avser hårdvaruprodukter som omfattas av denna förordning, såsom säkerhetsmoduler i maskinvara och mikroprocessorer, får kommissionen genom en genomförandeakt specificera hur EUCC ger en presumtion om överensstämmelse med de väsentliga kraven enligt bilaga I i denna förordning eller delar av dessa. En sådan genomförandeakt får specificera hur ett certifikat som utfärdas inom ramen för EUCC befriar tillverkaren från skyldigheten att genomföra en tredjepartsbedömning av överensstämmelse enligt denna förordning för de motsvarande kraven.

(41) I de fall då inga harmoniserade standarder antas, eller då de harmoniserade standarderna inte behandlar de väsentliga kraven i denna förordning på ett tillfredsställande sätt, bör kommissionen kunna anta gemensamma specifikationer genom genomförandeakter. Några exempel på skäl till att utveckla sådana gemensamma specifikationer i stället för att förlita sig på harmoniserade standarder är ett avslag på en begäran om standardisering från någon av de europeiska standardiseringsorganisationerna, onödiga förseningar i fastställandet av lämpliga harmoniserade standarder eller utarbetade standarders bristande överensstämmelse med kraven i denna förordning eller med kommissionens begäran. För att underlätta bedömningen av överensstämmelse med de väsentliga krav som fastställs i denna förordning bör det finnas en presumtion om överensstämmelse för produkter med digitala element som överensstämmer med de gemensamma specifikationer som antas av kommissionen i enlighet med denna förordning i syfte att formulera detaljerade tekniska specifikationer av dessa krav.

(42) Tillverkarna bör utarbeta en EU-försäkran om överensstämmelse för att tillhandahålla den information som krävs enligt denna förordning vad gäller produkter med digitala elements överensstämmelse med de väsentliga kraven i denna förordning och, om tillämpligt, med andra relevanta bestämmelser i unionens harmoniseringslagstiftning som omfattar produkten. Tillverkarna kan också åläggas att upprätta en EU-försäkran om överensstämmelse genom annan unionslagstiftning. För att säkerställa effektiv tillgång till information för marknadskontrolländamål bör en enda EU-försäkran om överensstämmelse upprättas med avseende på överensstämmelsen med alla berörda unionsakter. För att minska den administrativa bördan för ekonomiska aktörer bör

denna enda EU-försäkran om överensstämmelse kunna utgöras av dokumentation bestående av enskilda relevanta försäkringar om överensstämmelse.

(43) CE-märkningen visar att en produkt uppfyller kraven och utgör det synliga resultatet av en hel process, som omfattar en bedömning av överensstämmelse i vid bemärkelse. De allmänna principerna för CE-märkning fastställs i Europaparlamentets och rådets förordning (EG) nr 765/2008[18]. Bestämmelser för hur CE-märkningen ska anbringas på produkter med digitala element bör fastställas i denna förordning. CE-märkningen bör vara den enda märkning som garanterar överensstämmelse med kraven i denna förordning för produkter med digitala element.

(44) Det är nödvändigt att föreskriva förfaranden för bedömning av överensstämmelse, för att de ekonomiska aktörerna ska kunna visa överensstämmelse med de väsentliga krav som fastställs i denna förordning och marknadskontrollmyndigheterna ska kunna säkerställa att de produkter med digitala element som tillhandahålls på marknaden uppfyller dessa krav. Genom Europaparlamentets och rådets beslut nr 768/2008/EG[19] fastställs moduler för bedömning av överensstämmelse som står i proportion till risknivån och den säkerhetsnivå som krävs. För att säkerställa enhetlighet mellan olika sektorer och undvika ad hoc-varianter baseras förfarandena för bedömning av överensstämmelse för att kontrollera överensstämmelse med de väsentliga kraven i denna förordning för produkter med digitala element på dessa moduler. Förfarandena för bedömning av överensstämmelse bör omfatta granskning och kontroll av både produkten och processrelaterade krav som omfattar hela livscykeln för produkter med digitala element, inbegripet planering, utformning, utveckling eller produktion, testning och underhåll av produkten.

(45) I regel bör bedömningen av överensstämmelse för produkter med digitala element utföras av tillverkaren på eget ansvar i enlighet med ett förfarande baserat på modul A i beslut 768/2008/EG. Tillverkaren bör även fortsättningsvis ha flexibilitet att välja ett striktare förfarande för bedömning av överensstämmelse som involverar tredje part. Om produkten klassificeras som en kritisk produkt i klass I bör ytterligare kvalitetssäkring krävas för att visa överensstämmelsen med de väsentliga kraven i denna förordning. Tillverkaren bör tillämpa harmoniserade standarder, gemensamma specifikationer eller system för cybersäkerhetscertifiering enligt förordning (EU) 2019/881 som har identifierats av kommissionen i en genomförandeakt, om den vill utföra bedömningen av överensstämmelse på eget ansvar (modul A). Om tillverkaren inte använder sådana harmoniserade standarder, gemensamma specifikationer eller system för cybersäkerhetscertifiering bör tillverkaren genomgå bedömning av överensstämmelse med deltagande av tredje part. Med beaktande av den administrativa bördan för tillverkare och det faktum att cybersäkerheten har stor betydelse i utformnings- och utvecklingsfaserna för materiella och immateriella produkter med digitala element, har förfaranden för bedömning av överensstämmelse som baseras på modul B+C eller modul H i beslut 768/2008/EG valts som mest lämpliga för en proportionell och ändamålsenlig bedömning av överensstämmelse för kritiska produkter med digitala element. Tillverkare som genomför en tredjepartsbedömning av överensstämmelse kan välja det förförande som bäst passar den egna utformnings- och produktionsprocessen. Med tanke på de allt större

[18] Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och upphävande av förordning (EEG) nr 339/93 (EUT L 218, 13.8.2008, s. 30).

[19] Europaparlamentets och rådets beslut nr 768/2008/EG av den 9 juli 2008 om en gemensam ram för saluföring av produkter och upphävande av rådets beslut 93/465/EEG (EUT L 218, 13.8.2008, s. 82).

cybersäkerhetsrisker som är förbundna med användningen av produkter som klassificeras som kritiska klass II-produkter bör bedömningen av överensstämmelse alltid involvera en tredje part när det gäller dessa.

(46) Medan skapandet av materiella produkter med digitala element vanligtvis innebär att tillverkaren måste göra stora ansträngningar under hela utformnings-, utvecklings- och produktionsfaserna, fokuserar skapandet av produkter med digitala element i form av programvara nästan uteslutande på utformning och utveckling, medan produktionsfasen är mindre framträdande. I många fall måste dock programvaruprodukter ändå kompileras, byggas, förpackas, göras tillgängliga för nedladdning eller kopieras till fysiska medier innan de släpps ut på marknaden. Dessa aktiviteter bör anses som aktiviteter som motsvarar produktion vid tillämpningen av relevanta moduler för bedömning av överensstämmelse för att kontrollera överensstämmelsen med de väsentliga kraven i denna förordning under hela utformnings-, utvecklings- och produktionsfaserna för produkter med digitala element.

(47) För genomförandet av tredjepartsbedömningar av överensstämmelse för produkter med digitala element bör organ för bedömning av överensstämmelse anmälas av de nationella anmälande myndigheterna till kommissionen och övriga medlemsstater, under förutsättning att de uppfyller ett antal krav, i synnerhet vad gäller oberoende, kompetens och avsaknad av intressekonflikter.

(48) För att säkerställa en enhetlig kvalitetsnivå vid bedömning av överensstämmelse för produkter med digitala element måste också krav fastställas för de anmälande myndigheterna och andra organ som är involverade i bedömningen, anmälan och övervakningen av anmälda organ. Det system som fastställs i denna förordning bör kompletteras av ackrediteringssystemet enligt förordning (EG) nr 765/2008. Eftersom ackreditering är ett oumbärligt verktyg för att kontrollera kompetensen hos organen för bedömning av överensstämmelse bör det också användas för anmälningssyften.

(49) De nationella myndigheterna inom unionen bör betrakta öppen ackreditering enligt förordning (EG) nr 765/2008 som det bästa sättet att styrka den tekniska kompetensen hos organen för bedömning av överensstämmelse, för att säkerställa den nödvändiga nivån av förtroendet för intyg om överensstämmelse. Nationella myndigheter kan emellertid anse att de har tillräckliga möjligheter att utföra bedömningen på egen hand. I så fall bör de nationella myndigheterna, för att trygga en rimlig trovärdighetsnivå på bedömningar utförda av andra nationella myndigheter, ta fram den dokumentation som krävs för att visa kommissionen och övriga medlemsstater att de utvärderade organen för bedömning av överensstämmelse uppfyller de relevanta kraven.

(50) Organ för bedömning av överensstämmelse lägger ofta ut verksamhet kopplad till bedömningen av överensstämmelse på underentreprenad eller anlitar ett dotterbolag. För att se till att den erforderliga skyddsnivån uppfylls för produkter med digitala element som ska släppas ut på marknaden är det avgörande att underentreprenörer och dotterbolag uppfyller samma krav som de anmälda organen i fråga om utförandet av bedömning av överensstämmelse.

(51) Den anmälande myndigheten bör sända anmälan av ett organ för bedömning av överensstämmelse till kommissionen och övriga medlemsstater via databasen Nando. Nando är det elektroniska anmälningsverktyg som utvecklas och förvaltas av kommissionen och där man kan hitta en förteckning över alla anmälda organ.

(52) Eftersom de anmälda organen får erbjuda sina tjänster i hela unionen bör medlemsstaterna och kommissionen beredas tillfälle att göra invändningar rörande ett

anmält organ. Därför är det viktigt att en period fastställs under vilken eventuellt tvivel eller osäkerhet om kompetensen hos organen för bedömning av överensstämmelse kan redas ut innan de börjar fungera som anmälda organ.

(53) Av konkurrensskäl är det av avgörande betydelse att de anmälda organen tillämpar förfarandena för bedömning av överensstämmelse utan att belasta de ekonomiska aktörerna i onödan. Av samma skäl och för att säkerställa likabehandling av de ekonomiska aktörerna måste en enhetlig teknisk tillämpning av förfarandena för bedömning av överensstämmelse säkerställas. Detta bör bäst uppnås genom lämplig samordning och lämpligt samarbete mellan de anmälda organen.

(54) Marknadskontroll är ett viktigt verktyg för att säkerställa en korrekt och enhetlig tillämpning av unionslagstiftningen. En rättslig ram bör därför upprättas för ett ändamålsenligt genomförande av marknadskontroll. De regler om unionens marknadskontroll och kontroll av produkter som förs in på unionsmarknaden som föreskrivs i Europaparlamentets och rådets förordning (EU) 2019/1020[20] ärr tillämpliga på produkter med digitala element som omfattas av denna förordning.

(55) I enlighet med förordning (EU) 2019/1020 genomför marknadskontrollmyndigheterna marknadskontroll på medlemsstatens territorium. Denna förordning bör inte hindra medlemsstaterna från att välja vilka behöriga myndigheter som ska utföra dessa uppgifter. Varje medlemsstat bör utse en eller flera marknadskontrollmyndigheter på sitt territorium. Medlemsstaterna får välja att utse en befintlig eller en ny myndighet till att fungera som marknadskontrollmyndighet, inbegripet nationella behöriga myndigheter enligt artikel [artikel X] i direktiv [direktiv XXX/XXXX (NIS2)] eller utsedda nationella myndigheter för cybersäkerhetscertifiering enligt artikel 58 i förordning (EU) 2019/881. De ekonomiska aktörerna ska samarbeta fullt ut med marknadskontrollmyndigheterna och andra behöriga myndigheter. Varje medlemsstat bör underrätta kommissionen och övriga medlemsstater om sina marknadskontrollmyndigheter och behörighetsområdena för varje sådan myndighet och bör säkerställa de resurser och kompetenser som dessa behöver för att utföra sina kontrolluppgifter enligt denna förordning. I enlighet med artikel 10.2 och 10.3 i förordning (EU) 2019/1020 bör varje medlemsstat tillsätta ett centralt samordningskontor som bland annat ska ansvara för att representera en samordnad ståndpunkt från marknadskontrollmyndigheterna och bistå i samarbetet mellan marknadskontrollmyndigheterna i olika medlemsstater.

(56) En särskild administrativ samarbetsgrupp (Adco-grupp) bör inrättas för en enhetlig tillämpning av denna förordning, i enlighet med artikel 30.2 i förordning (EU) 2019/1020. Adco-gruppen bör bestå av representanter för de nationella marknadskontrollmyndigheterna och, om så är lämpligt, representanter för de centrala samordningskontoren. Kommissionen bör stödja och uppmuntra samarbete mellan marknadskontrollmyndigheter genom unionsnätverket för produktöverensstämmelse, som inrättats på grundval av artikel 29 i förordning (EU) 2019/1020 och som består av representanter från varje medlemsstat, inbegripet en representant för varje centralt samordningskontor som avses i artikel 10 i förordning (EU) 2019/1020 och en valfri nationell expert, ordförandena för Adco-grupperna och representanter för kommissionen. Kommissionen bör delta i nätverkets, dess undergruppers och denna

[20] Europaparlamentets och rådets förordning (EU) 2019/1020 av den 20 juni 2019 om marknadskontroll och överensstämmelse för produkter och om ändring av direktiv 2004/42/EG och förordningarna (EG) nr 765/2008 och (EU) nr 305/2011 (EUT L 169, 25.6.2019, s. 1).

Adco-grupps möte. Den bör också bistå denna Adco-grupp genom ett verkställande sekretariat som tillhandahåller tekniskt och logistiskt stöd.

(57) För att säkerställa att proportionella och effektiva åtgärder vidtas i rätt tid när det gäller produkter med digitala element som utgör en betydande cybersäkerhetsrisk bör det finnas ett unionsförfarande för skyddsåtgärder som innebär att berörda parter underrättas om åtgärder som är planerade att vidtas för sådana produkter. På så sätt kan också marknadskontrollmyndigheterna få möjlighet att, i samarbete med de berörda ekonomiska aktörerna, agera i ett tidigare skede när det är nödvändigt. Om medlemsstaterna och kommissionen är överens om att en medlemsstats åtgärd är berättigad, bör kommissionen inte involveras ytterligare, utom i de fall då den bristande överensstämmelsen kan anses bero på brister i en harmoniserad standard.

(58) I vissa fall kan en produkt med digitala element som uppfyller kraven i denna förordning ändå utgöra en betydande cybersäkerhetsrisk eller utgöra en risk för människors hälsa eller säkerhet, för uppfyllandet av skyldigheter enligt sådan unionslagstiftning eller nationell lagstiftning som är avsedd att skydda grundläggande rättigheter, tillgången till och autenticiteten, integriteten eller konfidentialiteten för tjänster som väsentliga entiteter av den typ som avses i [bilaga I till direktiv XXX/XXXX (NIS2)] erbjuder med användning av ett elektroniskt informationssystem eller för andra aspekter av skyddet av allmänintresset. Därför är det nödvändigt att fastställa regler som säkerställer att dessa risker minskas. Följaktligen bör marknadskontrollmyndigheterna vidta åtgärder för att ålägga den ekonomiska aktören att säkerställa att produkten inte längre utgör en sådan risk, att återkalla den eller att dra tillbaka den, beroende på risken. Så snart en marknadskontrollmyndighet begränsar eller förbjuder den fria rörligheten för en produkt på detta sätt bör medlemsstaten utan dröjsmål underrätta kommissionen och övriga medlemsstater om de provisoriska åtgärderna och motivera sitt beslut. Om en marknadskontrollmyndighet antar sådana åtgärder mot produkter som utgör en risk bör kommissionen utan dröjsmål inleda samråd med medlemsstaterna och berörda ekonomiska aktörer (en eller flera) samt utvärdera den nationella åtgärden. På grundval av utvärderingsresultaten bör kommissionen fastställa om den nationella åtgärden är motiverad eller inte. Kommissionen bör rikta beslutet till alla medlemsstater och omedelbart delge dem och de berörda ekonomiska aktörerna beslutet. Om åtgärden anses vara berättigad kan kommissionen också överväga att anta förslag om översyn av respektive unionslagstiftning.

(59) För produkter med digitala element som utgör en betydande cybersäkerhetsrisk, där det finns skäl att tro att dessa inte uppfyller kraven i denna förordning, eller för produkter som uppfyller kraven i denna förordning men som utgör andra viktiga risker, exempelvis risker för människors hälsa eller säkerhet, grundläggande rättigheter eller tillhandahållandet av tjänster av väsentliga entiteter av den typ som avses i [bilaga I till direktiv XXX / XXXX (NIS2)] kan kommissionen begära att Enisa gör en utvärdering. Baserat på denna utvärdering kan kommissionen genom genomförandeakter vidta korrigerande eller begränsande åtgärder på unionsnivå, inbegripet beslut om tillbakadragande från marknaden eller återkallande av respektive produkter, inom en rimlig tid i förhållande till typen av risk. Kommissionen får endast tillgripa en sådan åtgärd under exceptionella omständigheter som motiverar ett omedelbart ingripande för att bevara en välfungerande inre marknad och endast när inga verkningsfulla åtgärder har vidtagits av kontrollmyndigheterna för att åtgärda situationen, Sådana exceptionella omständigheter kan vara akutsituationer där exempelvis en tillverkare gör en produkt som inte uppfyller kraven allmänt tillgänglig

i flera medlemsstater och den även används i nyckelsektorer av entiteter som omfattas av [direktiv XXX / XXXX (NIS2)], och produkten samtidigt innehåller kända sårbarheter som utnyttjas av fientliga aktörer utan att tillverkaren tillhandahåller tillgängliga programfixar. Kommissionen får vid sådana akutsituationer ingripa endast under den tid som de exceptionella omständigheterna varar och om den bristande överensstämmelsen med denna förordning eller de betydande riskerna kvarstår.

(60) I de fall då det finns indikationer på bristande överensstämmelse med denna förordning i flera medlemsstater bör marknadskontrollmyndigheterna kunna genomföra gemensamma åtgärder med andra myndigheter för att kontrollera överensstämmelsen och identifiera cybersäkerhetsrisker för produkter med digitala element.

(61) Samtidiga samordnade kontrollåtgärder (*sweeps*) är särskilda kontrollåtgärder som vidtas av marknadskontrollmyndigheterna och som kan förbättra produktsäkerheten ytterligare. Dessa samordnade kontrollåtgärder bör i synnerhet vidtas när det finns marknadstrender, klagomål från konsumenter eller andra indikationer som tyder på att vissa produktkategorier ofta utgör cybersäkerhetsrisker. Enisa bör lämna förslag till marknadskontrollmyndigheterna på produktkategorier som kan omfattas av samtidiga samordnade kontrollåtgärder, baserat på bland annat de anmälningar om produktsårbarheter och incidenter som inkommer till Enisa.

(62) För att säkerställa att regelverket vid behov kan anpassas bör befogenheten att anta akter i enlighet med artikel 290 i fördraget delegeras till kommissionen när det gäller uppdatering av förteckningen över kritiska produkter i bilaga III och specificering av definitionerna av dessa produktkategorier. Befogenheten att anta akter i enlighet med den artikeln bör delegeras till kommissionen för att identifiera produkter med digitala element som omfattas av andra unionsregler som ger samma skyddsnivå som denna förordning och specificera om det skulle vara nödvändigt med några begränsningar eller uteslutanden från denna förordnings tillämpningsområde samt specificera sådana begränsningars omfattning, i förekommande fall. Befogenheten att anta akter i enlighet med den artikeln bör också delegeras till kommissionen med avseende på det potentiella kravet på certifiering av vissa mycket kritiska produkter med digitala element baserat på kritikalitetskriterier som fastställs i denna förordning, samt för att specificera minimiinnehållet i EU-försäkran om överensstämmelse och komplettera de aspekter som ska ingå i den tekniska dokumentationen. Det är särskilt viktigt att kommissionen genomför lämpliga samråd under sitt förberedande arbete, inklusive på expertnivå, och att dessa samråd genomförs i enlighet med principerna i det interinstitutionella avtalet om bättre lagstiftning av den 13 april 2016[21]. För att säkerställa lika stor delaktighet i förberedelsen av delegerade akter erhåller Europaparlamentet och rådet alla handlingar samtidigt som medlemsstaternas experter, och deras experter ges systematiskt tillträde till möten i kommissionens expertgrupper som arbetar med förberedelse av delegerade akter.

(63) För att säkerställa enhetliga villkor för genomförandet av denna förordning bör kommissionen tilldelas genomförandebefogenheter för att specificera formatet för och vad som ska ingå i programvaruförteckningen, ytterligare specificera typen av information, formatet och förfarandet för de anmälningar om aktivt utnyttjade sårbarheter och incidenter som lämnas till Enisa av tillverkarna, specificera de europeiska system för cybersäkerhetscertifiering som antas i enlighet med förordning

[21] EUT L 123, 12.5.2016, s. 1.

(EU) 2019/881 och som kan användas för att visa överensstämmelse med de väsentliga krav eller delar av dessa som fastställs i bilaga I till denna förordning, anta gemensamma specifikationer med avseende på de väsentliga krav som fastställs i bilaga I, fastställa tekniska specifikationer för piktogram eller andra märkningar relaterade till säkerheten för produkter med digitala element, och mekanismer för att främja användningen av sådana samt besluta om korrigerande eller begränsande åtgärder på unionsnivå vid exceptionella omständigheter som motiverar ett omedelbart ingripande för att bevara en välfungerande inre marknad. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011[22].

(64) För att säkerställa ett förtroendefullt och konstruktivt samarbete mellan marknadskontrollmyndigheter på unionsnivå och nationell nivå bör alla parter som är involverade i tillämpningen av denna förordning respektera konfidentialiteten för information och data som de erhåller i utförandet av sina uppgifter.

(65) För att säkerställa en effektiv efterlevnadskontroll av de skyldigheter som fastställs i denna förordning bör varje marknadskontrollmyndighet ha befogenhet att påföra eller begära påförande av administrativa sanktionsavgifter. Det bör därför fastställas maxnivåer för administrativa sanktionsavgifter som kommer att föreskrivas i nationell lagstiftning med avseende på bristande uppfyllande av de skyldigheter som fastställs i denna förordning. När det administrativa sanktionsbeloppet fastställs i varje enskilt fall bör alla relevanta omständigheter i den specifika situationen beaktas och som ett minimum de som uttryckligen fastställs i denna förordning, inbegripet huruvida andra marknadskontrollmyndigheter redan har påfört samma aktör administrativa sanktionsavgifter för liknande överträdelser. Sådana omständigheter kan antingen vara försvårande, i situationer där samma aktörs överträdelse fortsätter på territoriet för andra medlemsstater än den där den administrativa sanktionsavgiften redan har påförts, eller förmildrande, genom att säkerställa att eventuella administrativa sanktionsavgifter som övervägs av en annan marknadskontrollmyndighet för samma ekonomiska aktör eller samma typ av överträdelse redan bör beakta sanktioner som påförts i andra medlemsstater och storleken på dessa, tillsammans med andra relevanta särskilda omständigheter. I samtliga fall bör den kumulativa administrativa sanktionsavgift som marknadskontrollmyndigheter i flera medlemsstater kan påföra samma ekonomiska aktör för samma typ av överträdelse fastställas med iakttagande av proportionalitetsprincipen.

(66) Om administrativa sanktionsavgifter påförs personer som inte är ett företag, bör den behöriga myndigheten ta hänsyn till den allmänna inkomstnivån i medlemsstaten och personens ekonomiska situation, när den överväger lämplig sanktionsavgift. Det bör vara upp till medlemsstaterna att fastställa om och i vilken utsträckning myndigheter ska omfattas av administrativa sanktionsavgifter.

(67) I sina förbindelser med tredjeländer strävar EU efter att främja internationell handel med reglerade produkter. En mängd olika åtgärder kan vidtas för att främja handel, inbegripet flera rättsliga instrument såsom bilaterala (mellanstatliga) avtal om ömsesidigt erkännande (MRA) av bedömning av överensstämmelse och märkning av reglerade produkter. Avtal om ömsesidigt erkännande upprättas mellan unionen och tredjeländer som är på jämförbar teknisk utvecklingsnivå och har en jämförbar strategi

[22] Europaparlamentets och rådets förordning (EU) nr 182/2011 av den 16 februari 2011 om fastställande av allmänna regler och principer för medlemsstaternas kontroll av kommissionens utövande av sina genomförandebefogenheter (EUT L 55, 28.2.2011, s. 13).

för bedömning av överensstämmelse. Dessa avtal baseras på ett ömsesidigt godtagande av intyg, märkning om överensstämmelse och provningsrapporter som utfärdats av parternas organ för bedömning av överensstämmelse enligt varje parts lagstiftning. I dagsläget finns sådana avtal med flera länder. Avtalen ingås för ett antal specifika sektorer, som kan variera från ett land till ett annat. För att ytterligare främja handel, och med beaktande av att leveranskedjorna för produkter med digitala element är globala, får avtal om ömsesidigt erkännande av bedömning av överensstämmelse ingås av unionen i enlighet med artikel 218 i EUF-fördraget för produkter som regleras i denna förordning. Samarbete med partnerländer är också viktigt, för att stärka cyberresiliensen globalt, eftersom det långsiktigt kommer att bidra till att stärka cybersäkerhetsramen både inom och utanför EU.

(68) Denna förordning bör med jämna mellanrum ses över av kommissionen i samråd med berörda parter, främst i syfte att avgöra behovet av ändringar mot bakgrund av samhällsutvecklingen, den politiska utvecklingen, den tekniska utvecklingen eller ändrade marknadsvillkor.

(69) De ekonomiska aktörerna bör ges tillräckligt med tid att anpassa sig till kraven i denna förordning. Förordningen bör börja tillämpas [24 månader] från ikraftträdandet, förutom skyldigheten att rapportera aktivt utnyttjade sårbarheter och incidenter, som bör börja tillämpas [12 månader] från denna förordnings ikraftträdande.

(70) Eftersom målet för denna förordning inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare, på grund av åtgärdens effekter, 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 detta mål.

(71) Europeiska datatillsynsmannen har hörts i enlighet med artikel 42.1 i Europaparlamentets och rådets förordning (EU) 2018/1725[23] och avgav ett yttrande den [...].

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

ALLMÄNNA BESTÄMMELSER

Artikel 1

Innehåll

I denna förordning fastställs

(a) regler för utsläppandet på marknaden av produkter med digitala element, för att säkerställa cybersäkerheten för sådana produkter,

[23] 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).

(b) väsentliga krav för utformningen, utvecklingen och tillverkningen av produkter med digitala element, och skyldigheter för ekonomiska aktörer när det gäller cybersäkerheten för dessa produkter,

(c) väsentliga krav för de processer för sårbarhetshantering som tillverkarna inför för att säkerställa cybersäkerheten för produkter med digitala element under hela deras livscykel samt skyldigheter för ekonomiska aktörer i samband med dessa processer, och

(d) regler för marknadskontroll och kontroll av efterlevnaden av ovannämnda regler och krav.

Artikel 2

Tillämpningsområde

1. Denna förordning är tillämplig på alla produkter med digitala element vars avsedda och rimligen förutsebara användning omfattar en direkt eller indirekt logisk eller fysisk dataanslutning till en enhet eller ett nät.

2. Förordningen är inte tillämplig på sådana produkter med digitala element som omfattas av följande unionsakter:

   (a) Förordning (EU) 2017/745.

   (b) Förordning (EU) 2017/746.

   (c) Förordning (EU) 2019/2144.

3. Denna förordning ska inte tillämpas på produkter med digitala element som har certifierats i enlighet med förordning (EU) 2018/1139.

4. Denna förordnings tillämpning på sådana produkter med digitala element som omfattas av andra unionsregler där krav fastställs avseende alla eller vissa risker som täcks av de väsentliga kraven i bilaga I får begränsas eller uteslutas om

   (a) sådana begränsningar eller uteslutanden är förenliga med den allmänna rättsliga ram som är tillämplig på dessa produkter, och

   (b) sektorsreglerna ger samma skyddsnivå som denna förordning.

   Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 50 för att ändra denna förordning genom att specificera om sådana begränsningar eller uteslutanden är nödvändiga, vilka produkter och regler som berörs samt begränsningens omfattning, i förekommande fall.

5. Denna förordning ska inte tillämpas på sådana produkter med digitala element som utvecklats uteslutande för ändamål som rör nationell säkerhet eller militära ändamål eller på produkter som utformats specifikt för att behandla säkerhetsskyddsklassificerade uppgifter.

Artikel 3

Definitioner

I denna förordning gäller följande definitioner:

(1) *produkt med digitala element*: programvaru- eller hårdvaruprodukt och dess lösningar för fjärrbehandling av data, inklusive programvaru- eller hårdvarukomponenter som släpps ut på marknaden separat.

(2) *fjärrbehandling av data*: databehandling på distans för vilken programvaran utformats och utvecklats av tillverkaren eller under tillverkarens ansvar, och vars avsaknad skulle innebära att produkten med digitala element inte kan utföra en av sina funktioner.

(3) *kritisk produkt med digitala element*: en produkt med digitala element som utgör en cybersäkerhetsrisk i enlighet med de kriterier som fastställs i artikel 6.2 och vars kärnfunktion fastställs i bilaga III.

(4) *mycket kritisk produkt med digitala element*: en produkt med digitala element som utgör en cybersäkerhetsrisk i enlighet med de kriterier som fastställs i artikel 6.5.

(5) *operativ teknik*: programbara digitala system eller enheter som interagerar med den fysiska miljön eller styr enheter som interagerar med den fysiska miljön.

(6) *programvara*: den del av ett elektroniskt informationssystem som utgörs av datorkod.

(7) *hårdvara*: ett fysiskt elektroniskt informationssystem, eller delar av ett sådant, som kan behandla, lagra eller överföra digitala data.

(8) *komponent*: programvara eller hårdvara som är avsedd att vara integrerad i ett elektroniskt informationssystem.

(9) *elektroniskt informationssystem*: system, inklusive elektrisk eller elektronisk utrustning, som kan behandla, lagra eller överföra digitala data.

(10) *logisk anslutning*: en virtuell representation av en dataförbindelse som genomförs via ett programvarugränssnitt.

(11) *fysisk anslutning*: varje anslutning mellan elektroniska informationssystem eller komponenter som genomförs med fysiska medel, inbegripet elektriska eller mekaniska gränssnitt, tråd eller radiovågor.

(12) *indirekt anslutning*: en anslutning till en enhet eller ett nät som inte sker direkt utan snarare som en del av ett större system som är direkt anslutningsbart till enheten eller nätet.

(13) *privilegium*: en åtkomsträtt som beviljas enskilda användare eller program för utförandet av säkerhetsrelevanta åtgärder inom ett elektroniskt informationssystem.

(14) *utökat privilegium*: en åtkomsträtt som beviljas enskilda användare eller program för utförandet av en utvidgad uppsättning säkerhetsrelevanta åtgärder inom ett elektroniskt informationssystem vilken, om den missbrukas eller komprometteras, skulle kunna göra det möjligt för en fientlig aktör att få en mer omfattande åtkomst till systemets eller organisationens resurser.

(15) *slutnod*: enhet som är ansluten till ett nät och som tjänar som ingångspunkt till det nätet.

(16) *nät- eller datorresurser*: data eller hårdvaru- eller programvarufunktioner som är tillgängliga antingen lokalt eller via ett nät eller annan ansluten enhet.

(17) *ekonomisk aktör*: tillverkaren, tillverkarens representant, importören, distributören eller varje annan fysisk eller juridisk person som omfattas av skyldigheter som fastställs i denna förordning.

(18) *tillverkare*: varje fysisk eller juridisk person som utvecklar eller tillverkar produkter med digitala element, eller som låter utforma, utveckla eller tillverka produkter med digitala element, och saluför dessa under eget namn eller varumärke, antingen mot betalning eller kostnadsfritt.

(19) *tillverkarens representant*: en fysisk eller juridisk person som är etablerad inom unionen och som enligt skriftlig fullmakt från en tillverkare har rätt att i dennes ställe utföra specificerade uppgifter.

(20) *importör*: en fysisk eller juridisk person som är etablerad i unionen och som på marknaden släpper ut en produkt med digitala element vilken bär namnet på eller varumärket för en fysisk eller juridisk person som är etablerad utanför unionen.

(21) *distributör*: en fysisk eller juridisk person i leveranskedjan, utöver tillverkaren eller importören, som tillhandahåller en produkt med digitala element på unionsmarknaden utan att påverka dess egenskaper.

(22) *utsläppande på marknaden*: tillhandahållande för första gången av en produkt med digitala element på unionsmarknaden.

(23) *tillhandahållande på marknaden*: varje leverans av en produkt med digitala element för distribution eller användning på unionsmarknaden i samband med kommersiell verksamhet, antingen mot betalning eller kostnadsfritt.

(24) *avsett ändamål*: den användning för vilken en produkt med digitala element är avsedd av leverantören, inbegripet det specifika sammanhanget och de specifika användningsvillkoren, enligt specifikationerna i de uppgifter som leverantören tillhandahåller i instruktioner till användaren, reklam- eller försäljningsmaterial och uttalanden samt i den tekniska dokumentationen.

(25) *rimligen förutsebar användning*: användning som inte nödvändigtvis är det avsedda ändamål som tillverkaren anger i instruktionerna till användaren, reklam- eller försäljningsmaterial och uttalanden eller i den tekniska dokumentationen, men som är den sannolika följden av rimligen förutsebart mänskligt beteende eller tekniska åtgärder eller interaktioner.

(26) *rimligen förutsebar felaktig användning*: användning av en produkt med digitala element på ett sätt som inte överensstämmer med dess avsedda ändamål, men som kan vara resultatet av rimligen förutsebart mänskligt beteende eller interaktion med andra system.

(27) *anmälande myndighet*: den nationella myndighet som ansvarar för inrättandet och genomförandet av de förfaranden som krävs för bedömning, utseende och anmälan av organ för bedömning av överensstämmelse och för övervakning av dessa.

(28) *bedömning av överensstämmelse*: processen där det kontrolleras om de väsentliga kraven i bilaga I har uppfyllts.

(29) *organ för bedömning av överensstämmelse*: ett organ enligt definitionen i artikel 2.13 i förordning (EU) nr 765/2008.

(30) *anmält organ*: organ för bedömning av överensstämmelse som utsetts i enlighet med artikel 33 i denna förordning och andra relevanta bestämmelser i unionens harmoniseringslagstiftning .

(31) *väsentlig ändring*: en ändring av produkten med digitala element efter dess utsläppande på marknaden, vilken påverkar produktens överensstämmelse med de väsentliga kraven i avsnitt 1 i bilaga I eller leder till en ändring av det avsedda ändamål för vilket produkten har bedömts.

(32) *CE-märkning*: märkning genom vilken en tillverkare anger att en produkt med digitala element och de processer som införts av tillverkaren överensstämmer med de väsentliga kraven i bilaga I och annan tillämplig unionslagstiftning som harmoniserar

villkoren för saluföring av produkter (*unionens harmoniseringslagstiftning*) och som föreskriver sådan märkning.

(33) *marknadskontrollmyndighet*: myndighet enligt definitionen i artikel 3.4 i förordning (EU) 2019/1020.

(34) *harmoniserad standard*: harmoniserad standard enligt definitionen i artikel 2.1 c i förordning (EU) nr 1025/2012.

(35) *cybersäkerhetsrisk*: risk enligt artikel [artikel X] i direktiv [direktiv XXX/XXXX (NIS2)].

(36) *betydande cybersäkerhetsrisk*: en cybersäkerhetsrisk som, baserat på dess tekniska egenskaper, kan antas innebära en hög sannolikhet för en incident som kan medföra allvarliga negativa konsekvenser, exempelvis genom att orsaka betydande materiell eller immateriell förlust eller störning.

(37) *programvaruförteckning*: en formell förteckning med närmare uppgifter om och leveranskedjeförhållanden för komponenter som ingår i programvaruelementen i en produkt med digitala element.

(38) *sårbarhet*: sårbarhet enligt artikel [artikel X] i direktiv [direktiv XXX/XXXX (NIS2)].

(39) *aktivt utnyttjad sårbarhet*: sårbarhet för vilken det finns tillförlitliga bevis på att en aktör använt en skadlig kod på ett system utan tillstånd från systemets ägare.

(40) *personuppgifter*: personuppgifter enligt definitionen i artikel 4.1 i förordning (EU) 2016/679.

Artikel 4

Fri rörlighet

1. Medlemsstaterna får inte, med hänvisning till aspekter som omfattas av denna förordning, hindra att produkter med digitala element som överensstämmer med kraven i denna förordning tillhandahålls på marknaden.

2. Medlemsstaterna får inte förhindra att sådana produkter med digitala element som inte uppfyller kraven i denna förordning visas och används vid mässor, utställningar och demonstrationer eller liknande evenemang.

3. Medlemsstaterna får inte förhindra att ej färdigställd programvara som inte uppfyller kraven i denna förordning tillhandahålls, under förutsättning att programvaran endast tillhandahålls under den begränsade tid som krävs för testningsändamål och att en synlig märkning tydligt anger att den inte uppfyller kraven i denna förordning och att den inte kommer att tillhandahållas på marknaden för andra ändamål än testning.

Artikel 5

Krav för produkter med digitala element

Produkter med digitala element får endast tillhandahållas på marknaden om

(1) de uppfyller de väsentliga kraven i avsnitt 1 i bilaga I, förutsatt att de är korrekt installerade och underhållna och används för avsett ändamål eller under förhållanden som rimligen kan förutses och, i tillämpliga fall, uppdateras, och

(2) de processer som införs av tillverkaren uppfyller de väsentliga krav som fastställs i avsnitt 2 i bilaga I.

Artikel 6

Kritiska produkter med digitala element

1. Produkter med digitala element som tillhör en kategori som förtecknas i bilaga III ska anses som kritiska produkter med digitala element. Produkter vars kärnfunktioner tillhör en kategori som förtecknas i bilaga III till denna förordning ska anses ingå i den kategorin. Kategorier av kritiska produkter med digitala element ska indelas i klass I och klass II enligt bilaga III, baserat på produktens cybersäkerhetsrisknivå.

2. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 50 för att ändra bilaga III genom att införa en ny kategori i förteckningen över kategorier av kritiska produkter med digitala element eller stryka en befintlig kategori från förteckningen. När kommissionen bedömer behovet av en ändring av förteckningen i bilaga III ska den ta hänsyn till cybersäkerhetsrisknivån för den berörda kategorin av produkter med digitala element. Vid fastställandet av cybersäkerhetsrisknivån ska ett eller flera av följande kriterier beaktas:

   (a) De cybersäkerhetsrelaterade funktionerna hos produkten med digitala element och om produkten har minst ett av följande attribut:

      (i) Den är utformad för att användas med utökat privilegium eller hantera privilegier.

      (ii) Den har direkt åtkomst eller privilegierad åtkomst till nätverks- eller datorresurser.

      (iii) Den är utformad för att kontrollera åtkomst till data eller operativ teknik.

      (iv) Den utför en funktion som är kritisk för förtroendet, i synnerhet sådana säkerhetsfunktioner som nätverkskontroll och säkerheten vid slutnoder samt nätskydd.

   (b) En avsedd användning i känsliga miljöer, däribland i industriell miljö eller användning av väsentliga entiteter av den typ som avses i bilaga [bilaga I] till direktiv [direktiv XXX/XXXX (NIS2)].

   (c) En avsedd användning för att utföra kritiska eller känsliga funktioner, såsom behandling av personuppgifter.

   (d) Den potentiella omfattningen av en negativ inverkan, särskilt i fråga om intensitet och förmåga att påverka en stor mängd personer.

   (e) I vilken utsträckning som användningen av produkter med digitala element redan har orsakat materiell eller immateriell förlust eller störning eller har gett upphov till betydande farhågor för att sådan negativ inverkan ska uppstå.

3. Kommissionen ges befogenhet att anta en delegerad akt i enlighet med artikel 50 för att komplettera denna förordning genom att specificera definitionerna av produktkategorierna i klasserna I och II enligt bilaga III. Den delegerade akten ska antas [senast 12 månader efter denna förordnings ikraftträdande].

4. Kritiska produkter med digitala element ska omfattas av de förfaranden för bedömning av överensstämmelse som avses i artikel 24.2 och 24.3.

5. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 50 för att komplettera denna förordning genom att specificera de kategorier av mycket kritiska produkter med digitala element för vilka tillverkarna ska vara skyldiga att erhålla ett europeiskt cybersäkerhetscertifikat inom ramen för ett europeiskt system för cybersäkerhetscertifiering i enlighet med förordning (EU) 2019/881, för att visa att de väsentliga krav som anges i bilaga I, eller delar av dem, uppfylls. Vid fastställandet av sådana kategorier av mycket kritiska produkter med digitala element ska kommissionen beakta cybersäkerhetsrisknivån för den berörda kategorin av produkter med digitala element, i ljuset av ett eller flera av de kriterier som anges i punkt 2 samt mot bakgrund av bedömningen av om denna produktkategori

   (a) används av eller krävs för väsentliga entiteter av den typ som avses i bilaga [bilaga I] till direktiv [direktiv XXX/ XXXX (NIS2)] eller kommer att ha en potentiell framtida betydelse för dessa entiteters aktiviteter, eller

   (b) har betydelse för resiliensen mot störande händelser i den totala leveranskedjan för produkter med digitala element.

Artikel 7

Allmän produktsäkerhet

Som avvikelse från artikel 2.1 tredje stycket b i förordning [förordningen om allmän produktsäkerhet], ska kapitel III avsnitt 1, kapitel V och VII samt kapitel IX–XI i förordning [förordningen om allmän produktsäkerhet] tillämpas på produkter med digitala element med avseende på säkerhetsrisker som inte omfattas av denna förordning, om produkterna inte omfattas av särskilda krav i andra bestämmelser i unionens harmoniseringslagstiftning i den mening som avses i [artikel 3.25 i förordningen om allmän produktsäkerhet].

Artikel 8

AI-system med hög risk

1. Produkter med digitala element som klassificeras som AI-system med hög risk i enlighet med artikel [artikel 6] i förordning [AI-förordningen] vilka omfattas av denna förordning och uppfyller de väsentliga krav som fastställs i avsnitt 1 i bilaga I till denna förordning, och för vilka tillverkaren har infört processer som uppfyller de väsentliga krav som fastställs i avsnitt 2 i bilaga I, ska anses överensstämma med de cybersäkerhetskrav som fastställs i artikel [artikel 15] i förordning [AI-förordningen], utan att det påverkar tillämpningen av andra krav avseende noggrannhet och robusthet som ingår i ovannämnda artikel, och i den mån som uppnåendet av den skyddsnivå som föreskrivs i dessa krav visas genom en EU-försäkran om överensstämmelse som utfärdats i enlighet med denna förordning.

2. För de produkter och cybersäkerhetskrav som avses i punkt 1 ska det relevanta förfarande för bedömning av överensstämmelse som föreskrivs i artikel [artikel 43] i förordning [AI-förordningen] tillämpas. Vid denna bedömning ska anmälda organ som har rätt att kontrollera överensstämmelsen för AI-system med hög risk inom ramen för förordning [AI-förordningen] också ha rätt att kontrollera överensstämmelsen med kraven i bilaga I till denna förordning för AI-system med hög risk inom ramen för denna förordning, förutsatt att dessa anmälda organs uppfyllande av kraven i artikel 29 i denna förordning har bedömts i samband med anmälningsförfarandet inom ramen för förordning [AI-förordningen].

3. Som avvikelse från punkt 2 ska kritiska produkter med digitala element som förtecknas i bilaga III till denna förordning, vilka omfattas av de förfaranden för bedömning av överensstämmelse som avses i artikel 24.2 a, 24.2 b, 24.3 a och 24.3 b i denna förordning och som också klassificeras som AI-system med hög risk enligt artikel [artikel 6] i förordning [AI-förordningen] och omfattas av förfarandet för bedömning av överensstämmelse som grundar sig på intern kontroll enligt bilaga [bilaga VI] till förordning [AI-förordningen], genomgå de förfaranden för bedömning av överensstämmelse som föreskrivs i denna förordning i den mån som de väsentliga kraven i denna förordning berörs.

Artikel 9

Maskinprodukter

Maskinprodukter som omfattas av förordning [förordningen om maskinprodukter] och som är produkter med digitala element i den mening som avses i denna förordning, och för vilka en EU-försäkran om överensstämmelse har utfärdats på grundval av denna förordning, ska anses uppfylla de väsentliga hälso- och säkerhetskrav som fastställs i bilaga [bilaga III, avsnitt 1.1.9 och 1.2.1] till förordning [förordningen om maskinprodukter], vad gäller skydd mot förvanskning samt säkerhet och tillförlitlighet i kontrollsystemen, och i den mån som en EU-försäkran om överensstämmelse som utfärdats i enlighet med denna förordning visar att den skyddsnivå som föreskrivs i dessa krav uppnås.

KAPITEL II

EKONOMISKA AKTÖRERS SKYLDIGHETER

Artikel 10

Tillverkares skyldigheter

1. När en produkt med digitala element släpps ut på marknaden ska tillverkarna säkerställa att den har utformats, utvecklats och producerats i enlighet med de väsentliga krav som fastställs i avsnitt 1 i bilaga I.

2. För att fullgöra den skyldighet som fastställs i punkt 1 ska tillverkarna göra en bedömning av de cybersäkerhetsrisker som är förbundna med en produkt med digitala element och beakta resultatet av bedömningen under planerings-, utformnings-, utvecklings-, produktions-, leverans- och underhållsfaserna för en produkt med digitala element, för att minimera cybersäkerhetsriskerna, förhindra säkerhetsincidenter och minimera konsekvenserna av sådana incidenter, däribland vad gäller användarnas hälsa och säkerhet.

3. När en produkt med digitala element släpps ut på marknaden ska tillverkaren inkludera en bedömning av cybersäkerhetsriskerna i den tekniska dokumentationen enligt artikel 23 och bilaga V. För de produkter med digitala element som avses i artiklarna 8 och 24.4 och som också omfattas av andra unionsrättsakter får bedömningen av cybersäkerhetsriskerna ingå i den riskbedömning som krävs enligt respektive unionsrättsakt. I de fall då vissa väsentliga krav inte är tillämpliga på den salufördа produkten med digitala element ska tillverkaren inkludera en tydlig motivering i den dokumentationen.

4. För att fullgöra den skyldighet som fastställs i punkt 1 ska tillverkarna visa tillbörlig aktsamhet när de integrerar komponenter som kommer från tredje part i produkter med digitala element. De ska säkerställa att sådana komponenter inte komprometterar säkerheten för produkten med digitala element.

5. Tillverkaren ska systematiskt och på ett sätt som står i proportion till cybersäkerhetsriskernas art dokumentera relevanta cybersäkerhetsaspekter som rör produkten med digitala element, inbegripet sårbarheter de får kännedom om och all relevant information som tillhandahålls av tredje part samt, i förekommande fall, uppdatera riskbedömningen av produkten.

6. När en produkt med digitala element släpps ut på marknaden ska tillverkarna, under produktens förväntade livslängd eller en femårsperiod från utsläppandet på marknaden, beroende på vilken period som är kortast, säkerställa att produktens sårbarheter hanteras effektivt och i enlighet med de väsentliga krav som fastställs i avsnitt 2 i bilaga I.

   Tillverkarna ska ha lämpliga policyer och förfaranden, inbegripet samordnade policyer för information om sårbarheter, enligt avsnitt 2.5 i bilaga I, för att behandla och åtgärda de potentiella sårbarheter i produkter med digitala element som rapporterats av interna eller externa källor.

7. Innan en produkt med digitala element släpps ut på marknaden ska tillverkarna sammanställa den tekniska dokumentation som avses i artikel 23.

   De ska genomföra de valda förfaranden för bedömning av överensstämmelse som avses i artikel 24 eller se till att de genomförs.

   När det genom detta förfarande för bedömning av överensstämmelse har visats att produkten med digitala element uppfyller de väsentliga kraven i avsnitt 1 i bilaga I och att de processer som tillverkaren infört uppfyller de väsentliga kraven i avsnitt 2 i bilaga I, ska tillverkarna upprätta EU-försäkran om överensstämmelse i enlighet med artikel 20 och anbringa CE-märkningen i enlighet med artikel 22.

8. Tillverkarna ska kunna uppvisa den tekniska dokumentationen och EU-försäkran om överensstämmelse, i förekommande fall, för marknadskontrollmyndigheterna i tio år efter det att produkten med digitala element har släppts ut på marknaden.

9. Tillverkarna ska säkerställa att det finns förfaranden som säkerställer att produkter med digitala element som är en del av serietillverkning fortsätter att överensstämma med kraven. Tillverkaren ska på lämpligt sätt ta hänsyn till förändringar i utvecklings- och tillverkningsprocessen eller i utformningen eller egenskaperna för produkten med digitala element samt till ändringar av de harmoniserade standarderna, de europeiska systemen för cybersäkerhetscertifiering eller de gemensamma specifikationer som avses i artikel 19 med hänvisning till vilka överensstämmelsen för produkten med digitala element försäkras eller genom vars tillämpning överensstämmelsen kontrolleras.

10. Tillverkarna ska säkerställa att produkter med digitala element åtföljs av information och instruktioner till användaren enligt bilaga II i elektronisk eller fysisk form. Sådan information och sådana instruktioner ska vara på ett språk som lätt kan förstås av användarna. De ska vara tydliga, lättbegripliga och lätt läsbara. De ska möjliggöra en säker installation, drift och användning av produkter med digitala element.

11. Tillverkarna ska antingen lämna en EU-försäkran om överensstämmelse tillsammans med produkten med digitala element, eller i instruktionerna till användaren och

informationen enligt bilaga II ange den webbadress där det går att få tillgång till EU-försäkran om överensstämmelse.

12. Från och med utsläppandet på marknaden och under produktens hela förväntade livslängd eller under en femårsperiod från utsläppandet på marknaden av en produkt med digitala element, beroende på vilken period som är kortast, ska en tillverkare som vet eller har skäl att tro att produkten med digitala element eller de processer som införts av tillverkaren inte överensstämmer med de väsentliga kraven i bilaga I omedelbart vidta de korrigerande åtgärder som krävs för att bringa produkten med digitala element eller tillverkarens processer i överensstämmelse eller dra tillbaka eller återkalla produkten, såsom lämpligt.

13. Tillverkarna ska på motiverad begäran av en marknadskontrollmyndighet förse denna med all information och dokumentation som behövs för att visa att produkten med digitala element och de processer som införts av tillverkaren överensstämmer med de väsentliga krav som fastställs i bilaga I, i pappersform eller i elektronisk form och på ett språk som lätt kan förstås av myndigheten. De ska samarbeta med marknadskontrollmyndigheten, på dess begäran, om alla åtgärder som vidtas för att undanröja de cybersäkerhetsrisker som den produkt med digitala element som de har släppt ut på marknaden utgör.

14. En tillverkare som upphör med sin verksamhet och därmed inte kan uppfylla de skyldigheter som fastställs i denna förordning ska, innan verksamheten upphör, underrätta de berörda marknadskontrollmyndigheterna om detta och även, i möjligaste mån och på alla tillgängliga sätt, underrätta användarna av de berörda produkterna med digitala element som släppts ut på marknaden.

15. Kommissionen får genom genomförandeakter specificera formatet och de aspekter som ska ingå i programvaruförteckningen enligt avsnitt 2.1 i bilaga I. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 51.2.

Artikel 11

Tillverkarnas rapporteringsskyldigheter

1. Tillverkaren ska, utan onödigt dröjsmål och under alla omständigheter senast 24 timmar efter att ha fått kännedom om en aktivt utnyttjad sårbarhet i en produkt med digitala element, anmäla detta till Enisa. Denna anmälan ska omfatta detaljerade uppgifter om sårbarheten och, i förekommande fall, de korrigerande eller riskreducerande åtgärder som vidtagits. Enisa ska utan onödigt dröjsmål, om det inte är motiverat av cybersäkerhetsriskrelaterade skäl, vidarebefordra denna anmälan till den CSIRT-enhet som av den berörda medlemsstaten utsetts för samordnad information om sårbarheter i enlighet med artikel [artikel X] i direktiv [direktiv XXX/XXXX (NIS2)] vid mottagandet och underrätta marknadskontrollmyndigheten om den anmälda sårbarheten.

2. Tillverkaren ska, utan onödigt dröjsmål och under alla omständigheter senast 24 timmar efter att ha fått kännedom om en incident som påverkar säkerheten för en produkt med digitala element, anmäla detta till Enisa. Enisa ska utan onödigt dröjsmål, om det inte är motiverat av cybersäkerhetsriskrelaterade skäl, vidarebefordra denna anmälan till den gemensamma kontaktpunkt som av den berörda medlemsstaten utsetts i enlighet med artikel [artikel X] i direktiv [direktiv XXX/XXXX (NIS2)] och underrätta marknadskontrollmyndigheten om den anmälda

incidenten. Incidentanmälan ska innehålla information om incidentens allvarlighetsgrad och konsekvenser och, i förekommande fall, ange om tillverkaren misstänker att incidenten orsakats av olagliga eller fientliga handlingar eller anser att den har gränsöverskridande konsekvenser.

3. Enisa ska lämna information som anmälts i enlighet med punkterna 1 och 2 till Europeiska kontaktnätverket för cyberkriser (EU-CyCLONe), som inrättats genom artikel [artikel X] i direktiv [direktiv XXX/XXXX (NIS2)], om informationen är relevant för den samordnade hanteringen av storskaliga cybersäkerhetsincidenter och -kriser på operativ nivå.

4. Tillverkaren ska, utan dröjsmål och efter att ha fått kännedom om incidenten, underrätta användarna av produkten med digitala element om incidenten och, vid behov, om korrigerande åtgärder som användaren kan vidta för att begränsa konsekvenserna av incidenten.

5. Kommissionen får genom genomförandeakter ytterligare specificera typen av information, formatet och förfarandet för anmälningar enligt punkterna 1 och 2. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 51.2.

6. På grundval av de anmälningar som inkommer i enlighet med punkterna 1 och 2 ska Enisa vartannat år utarbeta en teknisk rapport om nya trender i fråga om cybersäkerhetsrisker i produkter med digitala element, och lämna den till den samarbetsgrupp som avses i artikel [artikel X] i direktiv [direktiv XXX / XXXX (NIS2)]. Den första sådana rapporten ska lämnas in inom 24 månader från det att de skyldigheter som fastställs i punkterna 1 och 2 börjar gälla.

7. Tillverkarna ska när de identifierar en sårbarhet i en komponent, inbegripet en komponent med öppen källkod, som ingår i en produkt med digitala element, rapportera sårbarheten till den person eller entitet som underhåller komponenten.

Artikel 12

Tillverkarens representant

1. En tillverkare får genom skriftlig fullmakt utse en representant.

2. Skyldigheterna enligt artikel 10.1–10.7 första strecksatsen och artikel 10.9 får inte delegeras till tillverkarens representant.

3. Tillverkarens representant ska utföra de uppgifter som anges i fullmakten från tillverkaren. Fullmakten ska ge representanten rätt att minst göra följande:

   (a) Inneha den EU-försäkran om överensstämmelse som avses i artikel 20 och den tekniska dokumentation som avses i artikel 23 för att kunna uppvisa dem för marknadskontrollmyndigheterna i tio år efter det att produkten med digitala element har släppts ut på marknaden.

   (b) På motiverad begäran av en marknadskontrollmyndighet förse denna med all information och dokumentation som behövs för att visa överensstämmelsen för en produkt med digitala element.

   (c) På marknadskontrollmyndigheternas begäran samarbeta med dem om åtgärder som vidtas för att undanröja riskerna med en produkt med digitala element som omfattas av fullmakten.

Artikel 13

Importörers skyldigheter

1. Importörer får på marknaden endast släppa ut sådana produkter med digitala element som uppfyller de väsentliga kraven i avsnitt 1 i bilaga I och för vilka de processer som införts av tillverkaren uppfyller de väsentliga kraven i avsnitt 2 i bilaga I.

2. Innan en produkt med digitala element släpps ut på marknaden ska importörerna säkerställa att

   (a) de tillämpliga förfaranden för bedömning av överensstämmelse som avses i artikel 24 har genomförts av tillverkaren,

   (b) tillverkaren har upprättat den tekniska dokumentationen, och

   (c) produkten med digitala element är försedd med den CE-märkning som avses i artikel 22 och åtföljs av den information och de instruktioner till användaren som fastställs i bilaga II.

3. Om en importör anser eller har skäl att tro att en produkt med digitala element eller de processer som införts av tillverkaren inte överensstämmer med de väsentliga kraven i bilaga I, får importören inte släppa ut produkten på marknaden förrän produkten eller processerna som införts av tillverkaren har bringats till överensstämmelse med de väsentliga kraven i bilaga I. Om en produkt med digitala element utgör en betydande cybersäkerhetsrisk ska importören också underrätta tillverkaren och marknadskontrollmyndigheterna om detta.

4. På produkter med digitala element ska importörer ange namn, registrerat firmanamn eller registrerat varumärke samt postadress och e-postadress där de kan kontaktas eller, om detta inte är möjligt, ska detta anges på förpackningen eller i ett dokument som åtföljer produkten med digitala element. Kontaktuppgifterna ska vara på ett språk som lätt kan förstås av användarna och marknadskontrollmyndigheterna.

5. Importörerna ska säkerställa att produkten med digitala element åtföljs av de instruktioner till användaren och den information som fastställs i bilaga II på ett språk som lätt kan förstås av användarna.

6. Importörer som vet eller har skäl att tro att en produkt med digitala element som de har släppt ut på marknaden eller de processer som införts av tillverkaren inte överensstämmer med de väsentliga kraven i bilaga I ska omedelbart vidta de korrigerande åtgärder som krävs för att bringa produkten med digitala element eller tillverkarens processer i överensstämmelse med de väsentliga kraven i bilaga I, eller dra tillbaka eller återkalla produkten, om så är lämpligt.

   När importörer identifierar en sårbarhet i en produkt med digitala element ska de utan dröjsmål underrätta tillverkaren om denna. Om en produkt med digitala element utgör en betydande cybersäkerhetsrisk ska importörerna dessutom omedelbart underrätta marknadskontrollmyndigheterna i de medlemsstater på vilkas marknad de har tillhandahållit produkten med digitala element, och lämna uppgifter om i synnerhet den bristande överensstämmelsen och de korrigerande åtgärder som vidtagits.

7. Under tio år efter det att produkten med digitala element har släppts ut på marknaden ska importörerna kunna uppvisa en kopia av EU-försäkran om överensstämmelse för marknadskontrollmyndigheterna och säkerställa att dessa myndigheter på begäran kan få tillgång till den tekniska dokumentationen.

8. Importörerna ska på motiverad begäran av en marknadskontrollmyndighet förse denna med all information och dokumentation som behövs för att visa att produkten med digitala element överensstämmer med de väsentliga krav som fastställs i avsnitt 1 i bilaga I och att de processer som införts av tillverkaren överensstämmer med de väsentliga krav som fastställs i avsnitt 2 i bilaga I, i pappersform eller i elektronisk form och på ett språk som lätt kan förstås av myndigheten. De ska på begäran samarbeta med den myndigheten om de åtgärder som vidtas för att undanröja de cybersäkerhetsrisker som den produkt med digitala element som de släppt ut på marknaden utgör.

9. När en importör av en produkt med digitala element får kännedom om att produktens tillverkare upphört med sin verksamhet och därmed inte kan uppfylla de skyldigheter som fastställs i denna förordning ska importören underrätta berörda marknadskontrollmyndigheter om detta och även, i möjligaste mån och på alla tillgängliga sätt, underrätta användarna av de produkter med digitala element som släppts ut på marknaden.

Artikel 14

Distributörers skyldigheter

1. När distributörerna tillhandahåller en produkt med digitala element på marknaden ska de agera med vederbörligt iakttagande av kraven i denna förordning.

2. Innan distributörerna tillhandahåller en produkt med digitala element på marknaden ska de kontrollera att

   (a) produkten med digitala element är försedd med CE-märkning,

   (b) tillverkaren och importören har uppfyllt de krav som anges i artiklarna 10.10, 10.11 och 13.4.

3. Om en distributör anser eller har skäl att tro att en produkt med digitala element eller de processer som införts av tillverkaren inte överensstämmer med de väsentliga kraven i bilaga I, får distributören inte tillhandahålla produkten på marknaden förrän produkten eller processerna som införts av tillverkaren har bringats till överensstämmelse. Om en produkt med digitala element utgör en betydande cybersäkerhetsrisk ska distributören underrätta tillverkaren och marknadskontrollmyndigheterna om detta.

4. Distributörer som vet eller har skäl att tro att en produkt med digitala element, som de har tillhandahållit på marknaden, eller de processer som införts av tillverkaren inte överensstämmer med de väsentliga kraven i bilaga I ska se till att de korrigerande åtgärder som krävs för att bringa produkten eller tillverkarens processer i överensstämmelse vidtas, eller dra tillbaka eller återkalla produkten, om så är lämpligt.

   När distributörer identifierar en sårbarhet i en produkt med digitala element ska de utan onödigt dröjsmål underrätta tillverkaren om denna. Om en produkt med digitala element utgör en betydande cybersäkerhetsrisk ska distributörerna dessutom omedelbart underrätta marknadskontrollmyndigheterna i de medlemsstater på vilkas marknad de har tillhandahållit produkten med digitala element, och lämna uppgifter om i synnerhet den bristande överensstämmelsen och de korrigerande åtgärder som vidtagits.

5. Distributörerna ska på motiverad begäran av en marknadskontrollmyndighet förse denna med all information och dokumentation som behövs för att visa att produkten med digitala element och de processer som införts av tillverkaren överensstämmer med de väsentliga krav som fastställs i bilaga I, i pappersform eller i elektronisk form och på ett språk som lätt kan förstås av myndigheten. De ska på begäran samarbeta med marknadskontrollmyndigheten om de åtgärder som vidtas för att undanröja de cybersäkerhetsrisker som den produkt med digitala element som de tillhandahåller på marknaden utgör.

6. När en distributör av en produkt med digitala element får kännedom om att produktens tillverkare upphört med sin verksamhet och därmed inte kan uppfylla de skyldigheter som fastställs i denna förordning ska distributören underrätta berörda marknadskontrollmyndigheter om detta och även, i möjligaste mån och på alla tillgängliga sätt, underrätta användarna av de produkter med digitala element som släppts ut på marknaden.

Artikel 15

Fall där tillverkares skyldigheter gäller för importörer och distributörer

En importör eller distributör ska anses som tillverkare enligt denna förordning och ska ha samma skyldigheter som tillverkaren enligt artiklarna 10, 11.1, 11.2, 11.4 och 11.7 om importören eller distributören släpper ut en produkt med digitala element på marknaden i eget namn eller under eget varumärke eller utför en väsentlig ändring av en produkt med digitala element som redan har släppts ut på marknaden.

Artikel 16

Andra fall där tillverkarnas skyldigheter gäller

En fysisk eller juridisk person, annan än tillverkaren, importören eller distributören, som utför en väsentlig ändring av en produkt med digitala element ska anses som tillverkare vid tillämpningen av denna förordning.

Denna person ska omfattas av tillverkarens skyldigheter enligt artiklarna 10, 11.1, 11.2, 11.4 och 11.7 när det gäller den del av produkten som påverkas av den väsentliga ändringen eller, om den väsentliga ändringen påverkar cybersäkerheten för produkten med digitala element som helhet, för hela produkten.

Artikel 17

Identifiering av ekonomiska aktörer

1. Ekonomiska aktörer ska, på begäran och om informationen finns tillgänglig, förse marknadskontrollmyndigheterna med följande information:

   (a) Namn och adress för ekonomiska aktörer som har levererat en produkt med digitala element till dem.

   (b) Namn och adress för ekonomiska aktörer som de har levererat en produkt med digitala element till.

2. De ekonomiska aktörerna ska kunna tillhandahålla den information som avses i punkt 1 i tio år efter det att de har fått en produkt med digitala element levererad och i tio år efter det att de har levererat en produkt med digitala element.

KAPITEL III

ÖVERENSSTÄMMELSE FÖR PRODUKTER MED DIGITALA ELEMENT

Artikel 18

Presumtion om överensstämmelse

1. Produkter med digitala element och processer som införts av tillverkaren som överensstämmer med harmoniserade standarder, eller delar av sådana, vilka har offentliggjorts i *Europeiska unionens officiella tidning*, ska förutsättas överensstämma med de väsentliga krav i bilaga I som omfattas av dessa standarder eller delar av dem.

2. Produkter med digitala element och processer som har införts av tillverkaren vilka överensstämmer med de gemensamma specifikationer som avses i artikel 19 ska förutsättas överensstämma med de väsentliga kraven i bilaga I, i den mån som de gemensamma specifikationerna täcker dessa krav.

3. Produkter med digitala element och processer som har införts av tillverkaren för vilka en EU-försäkran om överensstämmelse eller ett certifikat har utfärdats inom ramen för ett europeiskt system för cybersäkerhetscertifiering som införts i enlighet med förordning (EU) 2019/881 och specificerats enligt punkt 4, ska förutsättas överensstämma med de väsentliga kraven i bilaga I i den mån som EU-försäkran om överensstämmelse eller cybersäkerhetscertifikatet, eller delar av dessa, täcker dessa krav.

4. Kommissionen ges befogenhet att genom genomförandeakter specificera vilka europeiska system för cybersäkerhetscertifiering inom ramen för förordning (EU) 2019/881 som kan användas för att visa överensstämmelse med de väsentliga krav som fastställs i bilaga I, eller delar av dessa. I tillämpliga fall ska kommissionen också specificera om ett cybersäkerhetscertifikat som utfärdats inom ramen för sådana system befriar tillverkaren från skyldigheten att utföra en tredjepartsbedömning av överensstämmelse för de motsvarande kraven, i enlighet med artikel 24.2 a, 24.2 b, 24.3 a och 24.3 b. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 51.2.

Artikel 19

Gemensamma specifikationer

Om det inte finns några harmoniserade standarder enligt artikel 18 eller om kommissionen anser att de relevanta harmoniserade standarderna är otillräckliga för att uppfylla denna förordnings krav eller för att överensstämma med kommissionens standardiseringsbegäran, eller om det blir onödiga förseningar av standardiseringsförfarandet eller om kommissionens begäran om harmoniserade standarder inte har godtagits av de europeiska standardiseringsorganisationerna, ska kommissionen ges befogenhet att genom genomförandeakter anta gemensamma specifikationer med avseende på de väsentliga krav som fastställs i bilaga I. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 51.2.

Artikel 20

EU-försäkran om överensstämmelse

1. EU-försäkran om överensstämmelse ska upprättas av tillverkarna i enlighet med artikel 10.7 och ska ange att det har visats att de tillämpliga väsentliga kraven i bilaga I uppfylls.

2. EU-försäkran om överensstämmelse ska utformas i enlighet med mallen i bilaga IV och ska innehålla de uppgifter som anges i de relevanta förfaranden för bedömning av överensstämmelse som fastställs i bilaga VI. En sådan försäkran ska kontinuerligt uppdateras. Den ska tillhandahållas på det eller de språk som krävs av den medlemsstat där produkten med digitala element släpps ut eller tillhandahålls på marknaden.

3. Om en produkt med digitala element omfattas av mer än en unionsakt där det ställs krav på EU-försäkran om överensstämmelse ska en enda EU-försäkran om överensstämmelse upprättas med avseende på alla dessa unionsakter. I denna försäkran ska det anges vilka unionsakter som berörs, och det ska lämnas en publikationshänvisning till dem.

4. Genom att EU-försäkran om överensstämmelse upprättas ska tillverkaren ta ansvar för att produkten överensstämmer med kraven.

5. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 50 för att komplettera denna förordning genom att lägga till uppgifter till det minimiinnehåll för EU-försäkran om överensstämmelse som fastställs i bilaga IV, för att ta hänsyn till den tekniska utvecklingen.

Artikel 21

Allmänna principer för CE-märkning

CE-märkningen enligt artikel 3.32 ska omfattas av de allmänna principer som fastställs i artikel 30 i förordning (EG) nr 765/2008.

Artikel 22

Regler och villkor för anbringande av CE-märkning

1. CE-märkningen ska anbringas på produkten med digitala element så att den är synlig, läsbar och outplånlig. Om detta inte är möjligt eller inte är lämpligt på grund av produktens art, ska den anbringas på förpackningen och på den EU-försäkran om överensstämmelse enligt artikel 20 som medföljer produkten med digitala element. För produkter med digitala element i form av programvara ska CE-märkningen anbringas antingen på EU-försäkran om överensstämmelse enligt artikel 20 eller på den webbplats som åtföljer programvaruprodukten.

2. På grund av arten av produkt med digitala element får höjden på den CE-märkning som anbringas på produkten understiga 5 mm, förutsatt att den förblir synlig och läsbar.

3. CE-märkningen ska anbringas innan produkten med digitala element släpps ut på marknaden. Den får åtföljas av ett piktogram eller annan märkning som anger en särskild risk eller användning som fastställs i de genomförandeakter som avses i punkt 6.

4. CE-märkningen ska följas av det anmälda organets identifikationsnummer, i de fall då det organet är involverat i det förfarande för bedömning av överensstämmelse baserat på fullständig kvalitetssäkring (baserat på modul H) som avses i artikel 24.

Det anmälda organets identifikationsnummer ska anbringas av organet självt eller, enligt organets anvisningar, av tillverkaren eller tillverkarens representant.

5. Medlemsstaterna ska utgå från befintliga mekanismer för att säkerställa att bestämmelserna om CE-märkning tillämpas korrekt och vidta lämpliga åtgärder i händelse av otillbörlig användning av märkningen. I de fall då en produkt med digitala element omfattas av annan unionslagstiftning som också föreskriver CE-märkning ska CE-märkningen visa att produkten även uppfyller kraven i den lagstiftningen.

6. Kommissionen får genom genomförandeakter fastställa tekniska specifikationer för piktogram eller andra märkningar som rör säkerheten för produkter med digitala element, och mekanismer för att främja användningen av sådana. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 51.2.

Artikel 23

Teknisk dokumentation

1. Den tekniska dokumentationen ska omfatta alla relevanta data eller uppgifter om de metoder som tillverkaren använt för att säkerställa att produkter med digitala element och de processer som införts av tillverkaren uppfyller de väsentliga krav som fastställs i bilaga I. Den ska åtminstone omfatta de aspekter som fastställs i bilaga V.

2. Den tekniska dokumentationen ska upprättas innan produkten med digitala element släpps ut på marknaden och ska uppdateras kontinuerligt, vid behov, under produktens förväntade livslängd eller under en femårsperiod från produktens utsläppande på marknaden, beroende på vilken period som är kortast.

3. För de produkter med digitala element som avses i artiklarna 8 och 24.4 vilka även omfattas av andra unionsakter ska en enda teknisk dokumentation upprättas med den information som avses i bilaga V till denna förordning och den information som föreskrivs i respektive andra unionsakter.

4. Den tekniska dokumentation och korrespondens som avser förfaranden för bedömning av överensstämmelse ska upprättas på ett officiellt språk i den medlemsstat där det anmälda organet finns eller på ett språk som kan godtas av organet i fråga.

5. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 50 för att komplettera denna förordning med de aspekter som ska ingå i den tekniska dokumentationen enligt bilaga V för att ta hänsyn till den tekniska utvecklingen, samt utveckling som skett under denna förordnings genomförandeprocess.

Artikel 24

Förfaranden för bedömning av överensstämmelse för produkter med digitala element

1. Tillverkaren ska genomföra en bedömning av överensstämmelse avseende produkten med digitala element och de processer som införts av tillverkaren, där det ska fastställas om de väsentliga kraven i bilaga I uppfylls. Tillverkaren eller tillverkarens representant ska visa överensstämmelse med de väsentliga kraven genom att använda

   (a) förfarandet för intern kontroll (baserat på modul A) enligt bilaga VI, eller

(b) EU-typkontroll (baserat på modul B) enligt bilaga VI, följd av förfarandet för överensstämmelse med EU-typ grundat på intern tillverkningskontroll (baserat på modul C) enligt bilaga VI, eller

(c) överensstämmelse som grundar sig på fullständig kvalitetssäkring (baserat på modul H) enligt bilaga VI.

2. Vid bedömningen av om en kritisk produkt med digitala element i klass I enligt bilaga III och de processer som införts av dess tillverkare överensstämmer med de väsentliga kraven i bilaga I gäller att om tillverkaren eller tillverkarens representant inte har tillämpat – eller endast delvis har tillämpat – harmoniserade standarder, gemensamma specifikationer eller europeiska system för cybersäkerhetscertifiering enligt artikel 18, eller om sådana harmoniserade standarder, gemensamma specifikationer eller europeiska system för cybersäkerhetscertifiering saknas, ska den berörda produkten med digitala element och de processer som införts av tillverkaren genomgå ett av följande förfaranden med avseende på dessa väsentliga krav:

(a) EU-typkontroll (baserat på modul B) enligt bilaga VI, följd av förfarandet för överensstämmelse med EU-typ grundat på intern tillverkningskontroll (baserat på modul C) enligt bilaga VI, eller

(b) överensstämmelse som grundar sig på fullständig kvalitetssäkring (baserat på modul H) enligt bilaga VI.

3. Om produkten är en kritisk produkt med digitala element i klass II enligt bilaga III ska tillverkaren eller tillverkarens representant visa överensstämmelsen med de väsentliga kraven i bilaga I genom att använda ett av följande förfaranden:

(a) EU-typkontroll (baserat på modul B) enligt bilaga VI, följd av förfarandet för överensstämmelse med EU-typ grundat på intern tillverkningskontroll (baserat på modul C) enligt bilaga VI, eller

(b) överensstämmelse som grundar sig på fullständig kvalitetssäkring (baserat på modul H) enligt bilaga VI.

4. Tillverkare av produkter med digitala element som klassificeras som elektroniska patientjournalsystem inom ramen för förordning [förordningen om ett europeiskt hälsodataområde] ska visa överensstämmelse med de väsentliga krav som fastställs i bilaga I till denna förordning genom det relevanta förfarande för bedömning av överensstämmelse enligt förordning [kapitel III i förordningen om ett europeiskt hälsodataområde].

5. Anmälda organ ska ta hänsyn till små och medelstora företags särskilda intressen och behov när de fastställer avgifterna för bedömning av överensstämmelse och minska dessa avgifter i proportion till företagens specifika intressen och behov.

KAPITEL IV

ANMÄLAN AV ORGAN FÖR BEDÖMNING AV ÖVERENSSTÄMMELSE

Artikel 25

Anmälan

Medlemsstaterna ska till kommissionen och övriga medlemsstater anmäla vilka organ för bedömning av överensstämmelse som fått i uppdrag att utföra bedömningar av överensstämmelse i enlighet med denna förordning.

Artikel 26

Anmälande myndigheter

1. Medlemsstaterna ska utse en anmälande myndighet med ansvar för att inrätta och genomföra de förfaranden som krävs vid bedömning och anmälan av organ för bedömning av överensstämmelse och vid kontroll av anmälda organ, inklusive överensstämmelse med artikel 31.

2. Medlemsstaterna får bestämma att den bedömning och övervakning som avses i punkt 1 ska utföras av ett nationellt ackrediteringsorgan i den betydelse som anges i förordning (EG) nr 765/2008 och i enlighet därmed.

Artikel 27

Krav på anmälande myndigheter

1. En anmälande myndighet ska vara inrättad på ett sådant sätt att det inte uppstår någon intressekonflikt med organen för bedömning av överensstämmelse.

2. En anmälande myndighet ska vara organiserad och fungera på ett sådant sätt att dess verksamhet är objektiv och opartisk.

3. En anmälande myndighet ska vara organiserad på ett sådant sätt att alla beslut som rör anmälan av ett organ för bedömning av överensstämmelse fattas av annan behörig personal än den som utförde bedömningen.

4. En anmälande myndighet får inte erbjuda eller utföra sådan verksamhet som utförs av organ för bedömning av överensstämmelse eller konsulttjänster på kommersiell eller konkurrensmässig grund.

5. En anmälande myndighet ska skydda den konfidentiella information som den mottar.

6. En anmälande myndighet ska ha tillgång till tillräckligt med personal med lämplig kompetens för att korrekt kunna utföra sina uppgifter.

Artikel 28

Anmälande myndigheters informationsskyldighet

1. Medlemsstaterna ska informera kommissionen om sina förfaranden för bedömning och anmälan av organ för bedömning av överensstämmelse och för övervakning av anmälda organ samt om eventuella ändringar.

2. Kommissionen ska offentliggöra denna information.

Artikel 29

Krav på anmälda organ

1. För anmälning ska ett organ för bedömning av överensstämmelse uppfylla de krav som anges i punkterna 2–12.

2. Ett organ för bedömning av överensstämmelse ska inrättas i enlighet med nationell rätt och vara juridisk person.

3. Ett organ för bedömning av överensstämmelse ska vara ett tredjepartsorgan som är oberoende av den organisation eller produkt som den bedömer.

   Detta organ får vara ett organ som hör till en näringslivsorganisation eller branschorganisation som företräder företag som är involverade i utformning, utveckling, tillverkning, tillhandahållande, montering, användning eller underhåll av de produkter med digitala element som det bedömer, förutsatt att det kan styrkas att organet är oberoende och att intressekonflikter saknas.

4. Ett organ för bedömning av överensstämmelse, dess högsta ledning och den personal som ansvarar för utförandet av bedömningen av överensstämmelse får inte utgöras av den som utformar, utvecklar, tillverkar, levererar, installerar, köper, äger, använder eller underhåller de produkter med digitala element som bedöms och inte heller av en representant för någon av dessa parter. Detta ska inte hindra att bedömda produkter som är nödvändiga för verksamheten vid organet för bedömning av överensstämmelse används, eller att produkterna används för personligt bruk.

   Organ för bedömning av överensstämmelse, deras högsta ledning och den personal som ansvarar för utförandet av bedömningen av överensstämmelse får inte vara direkt inblandade i utformningen, utvecklingen, tillverkningen, marknadsföringen, installationen, användningen eller underhållet av dessa produkter, och inte heller representera parter som bedriver sådan verksamhet. De får inte delta i någon verksamhet som kan påverka deras objektivitet och integritet i samband med de bedömningar av överensstämmelse för vilka de har anmälts. Detta ska framför allt gälla konsulttjänster.

   Organ för bedömning av överensstämmelse ska säkerställa att deras dotterbolags eller underentreprenörers verksamhet inte påverkar konfidentialiteten, objektiviteten eller opartiskheten i organens bedömningar av överensstämmelse.

5. Organ för bedömning av överensstämmelse och deras personal ska utföra bedömningar av överensstämmelse med största möjliga yrkesintegritet, ha erforderlig teknisk kompetens på det specifika området och vara fria från alla påtryckningar och incitament, i synnerhet ekonomiska incitament, som kan påverka deras omdöme eller resultaten av deras bedömningar av överensstämmelse; detta gäller särskilt påtryckningar och incitament från personer eller grupper av personer som berörs av bedömningarnas resultat.

6. Ett organ för bedömning av överensstämmelse ska kunna utföra alla de uppgifter avseende bedömning av överensstämmelse som avses i bilaga VI och för vilka det har anmälts, oavsett om dessa uppgifter utförs av organet självt eller för dess räkning och under dess ansvar.

   Vid alla tidpunkter och vid varje bedömning av överensstämmelse och för varje typ eller kategori av produkt med digitala element för vilka det har anmälts ska organet för bedömning av överensstämmelse ha till sitt förfogande

   (a) personal med teknisk kunskap och tillräcklig och lämplig erfarenhet för att utföra de uppgifter som ingår i bedömningen av överensstämmelse,

   (b) beskrivningar av förfaranden enligt vilka bedömningar av överensstämmelse utförs; dessa beskrivningar ska säkerställa att förfarandena är transparenta och kan reproduceras. Organet ska ha lämpliga rutiner och förfaranden för att skilja

mellan de uppgifter som det utför i sin egenskap av anmält organ och annan verksamhet, och

(c) förfaranden som gör det möjligt för organet att utöva sin verksamhet med vederbörlig hänsyn tagen till ett företags storlek, bransch och struktur, den berörda produktteknikens komplexitet och eventuell mass- eller serietillverkning.

Det ska ha de nödvändiga medlen för att korrekt kunna utföra de tekniska och administrativa uppgifterna i samband med bedömningen av överensstämmelse och ha tillgång till den utrustning och de hjälpmedel som är nödvändiga.

7. Den personal som ansvarar för att utföra bedömningen av överensstämmelse ska ha

(a) fullgod teknisk och yrkesinriktad utbildning som täcker all slags bedömning av överensstämmelse för vilken organet för bedömning av överensstämmelse har anmälts,

(b) tillfredsställande kunskap om kraven för de bedömningar som de utför och befogenhet att utföra dessa bedömningar,

(c) tillräcklig kännedom och insikt om de väsentliga kraven, de tillämpliga harmoniserade standarderna och de relevanta bestämmelserna i unionens harmoniseringslagstiftning och dess genomförandeakter,

(d) förmåga att upprätta intyg, protokoll och rapporter som visar att bedömningarna har utförts.

8. Det ska garanteras att organen för bedömning av överensstämmelse, deras ledning och bedömningspersonal är opartiska.

Ersättningen till organets ledning och bedömningspersonal får inte vara beroende av antalet bedömningar som gjorts eller resultaten av bedömningarna.

9. Organ för bedömning av överensstämmelse ska vara ansvarsförsäkrade, om inte staten tar på sig ansvaret i enlighet med nationell rätt eller medlemsstaten själv tar direkt ansvar för bedömningen av överensstämmelse.

10. Personalen vid ett organ för bedömning av överensstämmelse ska iaktta tystnadsplikt beträffande all information som de erhåller vid utförandet av sina uppgifter enligt bilaga VI eller bestämmelser i nationell rätt som genomför den, utom gentemot marknadskontrollmyndigheterna i den medlemsstat där verksamheten bedrivs. Äganderätten ska vara skyddad. Organet för bedömning av överensstämmelse ska ha dokumenterade förfaranden som säkerställer uppfyllandet av kraven i denna punkt.

11. Organ för bedömning av överensstämmelse ska delta i, eller säkerställa att deras bedömningspersonal känner till, det relevanta standardiseringsarbetet och det arbete som utförs i samordningsgruppen för anmälda organ, som inrättats i enlighet med artikel 40, och de ska som generella riktlinjer använda de administrativa beslut och dokument som är resultatet av gruppens arbete.

12. Organen för bedömning av överensstämmelse ska fungera enligt konsekventa, rättvisa och rimliga villkor och bestämmelser och när det gäller avgifter särskilt beakta små och medelstora företags intressen.

Artikel 30

Presumtion om överensstämmelse för anmälda organ

För ett organ för bedömning av överensstämmelse som kan visa att det uppfyller kriterierna i de relevanta harmoniserade standarderna eller delar av dem till vilka hänvisningar har offentliggjorts i *Europeiska unionens officiella tidning* ska en presumtion om överensstämmelse med kraven i artikel 29 gälla, i den mån som dessa krav omfattas av de tillämpliga harmoniserade standarderna.

Artikel 31

Dotterbolag och underentreprenörer till anmälda organ

1. Om det anmälda organet lägger ut specifika uppgifter med anknytning till bedömningen av överensstämmelse på underentreprenad eller anlitar ett dotterbolag ska det säkerställa att underentreprenören eller dotterbolaget uppfyller kraven i artikel 29 och informera den anmälande myndigheten om detta.
2. De anmälda organen ska ta det fulla ansvaret för underentreprenörernas eller dotterbolagens uppgifter, oavsett var de är etablerade.
3. Verksamhet får läggas ut på underentreprenad eller utföras av ett dotterbolag endast om tillverkaren samtycker till det.
4. De anmälda organen ska se till att den anmälande myndigheten har tillgång till de relevanta dokumenten rörande bedömningen av underentreprenörens eller dotterbolagets kvalifikationer och det arbete som dessa har utfört i enlighet med denna förordning.

Artikel 32

Ansökan om anmälan

1. Ett organ för bedömning av överensstämmelse ska lämna in en ansökan om anmälan till den anmälande myndigheten i den medlemsstat där det är etablerat.
2. Ansökan ska åtföljas av en beskrivning av de bedömningar av överensstämmelse, det eller de förfaranden för bedömning av överensstämmelse och den eller de produkter som organet anser sig ha kompetens för samt ett ackrediteringsintyg, om det finns ett sådant, som utfärdats av ett nationellt ackrediteringsorgan och där det intygas att organet för bedömning av överensstämmelse uppfyller kraven i artikel 29.
3. Om organet för bedömning av överensstämmelse inte kan uppvisa något ackrediteringsbevis ska det ge den anmälande myndigheten alla de underlag som krävs för kontroll, erkännande och regelbunden tillsyn av att det uppfyller kraven i artikel 29.

Artikel 33

Anmälningsförfarande

1. De anmälande myndigheterna får endast anmäla de organ för bedömning av överensstämmelse som har uppfyllt kraven i artikel 29.
2. Den anmälande myndigheten ska underrätta kommissionen och de andra medlemsstaterna via databasen Nando som utvecklats och förvaltas av kommissionen.

3. Anmälan ska innehålla detaljerade uppgifter om bedömningarna av överensstämmelse, modulerna för bedömning av överensstämmelse och de berörda produkterna samt ett relevant intyg om kompetens.

4. Om en anmälan inte grundar sig på ett sådant ackrediteringsbevis som avses i artikel 32.2 ska den anmälande myndigheten ge kommissionen och de andra medlemsstaterna de skriftliga underlag som styrker att organet för bedömning av överensstämmelse har erforderlig kompetens och att de arrangemang som behövs för att säkerställa att organet övervakas regelbundet och fortsätter att uppfylla kraven i artikel 29 har inrättats.

5. Det berörda organet får bedriva verksamhet som anmält organ endast om kommissionen eller de andra medlemsstaterna inte har rest några invändningar inom två veckor från anmälan, i de fall då ett ackrediteringsintyg används, eller inom två månader från anmälan, i de fall då ingen ackreditering används.

   Endast ett sådant organ ska anses vara ett anmält organ vid tillämpning av denna förordning.

6. Kommissionen och övriga medlemsstater ska underrättas om eventuella relevanta senare ändringar av anmälan.

Artikel 34

Identifikationsnummer och förteckningar över anmälda organ

1. Kommissionen ska tilldela varje anmält organ ett identifikationsnummer.

   Organet ska tilldelas ett enda sådant nummer även om det anmälts enligt flera unionsakter.

2. Kommissionen ska offentliggöra förteckningen över de organ som anmälts enligt denna förordning, inklusive de identifikationsnummer som de har tilldelats och den verksamhet som de har anmälts för.

   Kommissionen ska säkerställa att denna förteckning hålls aktuell.

Artikel 35

Ändringar i anmälan

1. Om en anmälande myndighet har konstaterat eller har informerats om att ett anmält organ inte längre uppfyller de krav som anges i artikel 29 eller att det underlåter att fullgöra sina skyldigheter ska myndigheten i förekommande fall, beroende på hur allvarlig underlåtenheten att uppfylla kraven eller fullgöra skyldigheterna är, begränsa anmälan eller återkalla den tillfälligt eller slutgiltigt. Den ska omedelbart informera kommissionen och de andra medlemsstaterna om detta.

2. I händelse av begränsning eller tillfällig eller slutgiltig återkallelse av anmälan eller om det anmälda organet har upphört med verksamheten ska den anmälande medlemsstaten vidta lämpliga åtgärder för att säkerställa att det anmälda organets ärenden antingen behandlas av ett annat anmält organ eller hålls tillgängliga för de ansvariga anmälande myndigheterna och marknadskontrollmyndigheterna på deras begäran.

Artikel 36

Ifrågasättande av de anmälda organens kompetens

1. Kommissionen ska undersöka alla fall där den hyser tvivel, eller där den upplysts om sådana tvivel, om ett anmält organs kompetens eller ett anmält organs fortsatta uppfyllande av de krav och skyldigheter som det omfattas av.

2. Den anmälande medlemsstaten ska på begäran ge kommissionen all information om grunderna för anmälan eller det berörda organets fortsatta kompetens.

3. Kommissionen ska säkerställa att all känslig information som den erhåller under sina undersökningar behandlas konfidentiellt.

4. Om kommissionen konstaterar att ett anmält organ inte uppfyller eller inte längre uppfyller kraven för anmälan ska den meddela detta till den anmälande medlemsstaten och anmoda medlemsstaten att vidta erforderliga korrigerande åtgärder, t.ex. vid behov återta anmälan.

Artikel 37

De anmälda organens operativa skyldigheter

1. Anmälda organ ska utföra bedömningar av överensstämmelse i enlighet med förfarandena för bedömning av överensstämmelse i artikel 24 och bilaga VI.

2. Bedömningar av överensstämmelse ska utföras på ett proportionellt sätt så att de ej blir onödigt betungande för de ekonomiska aktörerna. Organ för bedömning av överensstämmelse ska utöva sin verksamhet med vederbörlig hänsyn till ett företags storlek, bransch och struktur, den berörda produktteknikens komplexitet och om produktionsprocessen karaktäriseras som mass- eller serietillverkning.

3. Anmälda organ ska dock iaktta den grad av noggrannhet och den skyddsnivå som krävs för att produkten ska överensstämma med kraven i denna förordning.

4. Om ett anmält organ konstaterar att en tillverkare inte uppfyller kraven i bilaga I eller motsvarande harmoniserade standarder eller gemensamma specifikationer som avses i artikel 19, ska det begära att tillverkaren vidtar lämpliga korrigerande åtgärder, och det ska inte utfärda ett intyg om överensstämmelse.

5. Om ett anmält organ vid övervakning av överensstämmelse efter det att ett intyg har utfärdats konstaterar att en produkt inte längre uppfyller kraven i denna förordning, ska det kräva att tillverkaren vidtar lämpliga korrigerande åtgärder, och vid behov ska intyget tillfälligt eller slutgiltigt återkallas.

6. Om korrigerande åtgärder inte vidtas eller inte får önskad effekt ska det anmälda organet, beroende på vad som är lämpligt, begränsa eller tillfälligt, alternativt slutgiltigt, återkalla alla intyg.

Artikel 38

De anmälda organens informationsskyldighet

1. De anmälda organen ska underrätta den anmälande myndigheten om följande:

   (a) Avslag på ansökan om intyg, eller begränsning, tillfälligt tillbakadragande eller återkallelse av ett intyg.

   (b) Omständigheter som inverkar på räckvidden och villkoren för anmälan.

(c) Begäran från marknadskontrollmyndigheterna om information om bedömningar av överensstämmelse.

(d) På begäran, bedömningar av överensstämmelse som gjorts inom ramen för anmälan och all annan verksamhet, inklusive gränsöverskridande verksamhet och underentreprenad.

2. De anmälda organen ska ge de andra organ som anmälts i enlighet med denna förordning, och som utför liknande bedömningar av överensstämmelse som täcker samma produkter, relevant information om frågor som rör negativa och, på begäran, positiva resultat av bedömningar av överensstämmelse.

Artikel 39

Utbyte av erfarenhet

Kommissionen ska se till att det förekommer utbyte av erfarenhet mellan de myndigheter i medlemsstaterna som ansvarar för riktlinjerna för anmälan.

Artikel 40

Samordning av anmälda organ

1. Kommissionen ska säkerställa att lämplig samordning och samarbete mellan de anmälda organen införs och att samordningen och samarbetet bedrivs på ett tillfredsställande sätt genom en sektorsövergripande grupp av anmälda organ.

2. Medlemsstaterna ska säkerställa att de organ som de har anmält deltar i gruppens arbete direkt eller genom utsedda företrädare.

KAPITEL V

MARKNADSKONTROLL OCH VERKSTÄLLIGHET

Artikel 41

Marknadskontroll och kontroll av produkter med digitala element på unionsmarknaden

1. Förordning (EU) 2019/1020 ska tillämpas på produkter med digitala element som omfattas av denna förordning.

2. Varje medlemsstat ska utse en eller flera marknadskontrollmyndigheter för att säkerställa ett effektivt genomförande av denna förordning. Medlemsstaterna får utse en befintlig eller en ny myndighet till att fungera som marknadskontrollmyndighet inom ramen för denna förordning.

3. När så är lämpligt ska marknadskontrollmyndigheterna samarbeta med de nationella myndigheter för cybersäkerhetscertifiering som utsetts i enlighet med artikel 58 i förordning (EU) 2019/881 och regelbundet utbyta information med dessa. När det gäller tillsynen över genomförandet av rapporteringsskyldigheterna enligt artikel 11 i denna förordning ska de utsedda marknadskontrollmyndigheterna samarbeta med Enisa.

4. När så är lämpligt ska marknadskontrollmyndigheterna samarbeta med andra marknadskontrollmyndigheter som utsetts på grundval av andra bestämmelser i

unionens harmoniseringslagstiftning för andra produkter och regelbundet utbyta information med dessa.

5. Marknadskontrollmyndigheterna ska vid behov samarbeta med de myndigheter som utövar tillsyn över unionens dataskyddslagstiftning. I detta samarbete ingår att underrätta dessa myndigheter om alla iakttagelser av betydelse för deras fullgörande av sina befogenheter, inbegripet utfärdande av vägledning och råd i enlighet med punkt 8 i denna artikel om vägledningen och råden rör behandling av personuppgifter.

   Myndigheter som utövar tillsyn över unionens dataskyddslagstiftning ska ha befogenhet att begära och få åtkomst till all dokumentation som skapas eller upprätthålls enligt denna förordning när de behöver åtkomst till sådan dokumentation för att utföra sina uppgifter. De ska underrätta de utsedda marknadskontrollmyndigheterna i den berörda medlemsstaten om varje sådan begäran.

6. Medlemsstaterna ska säkerställa att de utsedda marknadskontrollmyndigheterna har tillräckliga ekonomiska resurser och personalresurser för att kunna fullgöra sina uppgifter enligt denna förordning.

7. Kommissionen ska underlätta utbytet av erfarenhet mellan utsedda marknadskontrollmyndigheter.

8. Marknadskontrollmyndigheterna får ge ekonomiska aktörer vägledning och råd om genomförandet av denna förordning, med stöd av kommissionen.

9. Marknadskontrollmyndigheterna ska årligen rapportera resultaten av relevant marknadskontroll till kommissionen. De utsedda marknadskontrollmyndigheterna ska utan dröjsmål rapportera till kommissionen och berörda nationella konkurrensmyndigheter om all information som framkommit i samband med marknadskontrollen och som kan vara av potentiellt intresse för tillämpningen av unionens konkurrenslagstiftning.

10. För produkter med digitala element som omfattas av denna förordning och som klassificeras som AI-system med hög risk i enlighet med artikel [artikel 6] i förordning [AI-förordningen] ska de marknadskontrollmyndigheter som utsetts inom ramen för förordning [AI-förordningen] vara de myndigheter som ansvarar för den marknadskontroll som föreskrivs i denna förordning. De marknadskontrollmyndigheter som utsetts i enlighet med förordning [AI-förordningen] ska vid behov samarbeta med de marknadskontrollmyndigheter som utsetts i enlighet med denna förordning och, när det gäller tillsyn över genomförandet av rapporteringsskyldigheten enligt artikel 11, med Enisa. De marknadskontrollmyndigheter som utsetts i enlighet med förordning [AI-förordningen] ska i synnerhet underrätta de marknadskontrollmyndigheter som utsetts i enlighet med denna förordning om alla iakttagelser av betydelse för fullgörandet av deras uppgifter förbundna med genomförandet av denna förordning.

11. En särskild administrativ samarbetsgrupp (Adco-grupp) ska inrättas för en enhetlig tillämpning av denna förordning, i enlighet med artikel 30.2 i förordning (EU) 2019/1020. Adco-gruppen ska bestå av företrädare för de utsedda marknadskontrollmyndigheterna och, om så är lämpligt, företrädare för de centrala samordningskontoren.

Artikel 42

Tillgång till data och dokumentation

När det behövs för att bedöma överensstämmelsen med de väsentliga kraven i bilaga I för produkter med digitala element och de processer som införts av tillverkarna, och på motiverad begäran, ska marknadskontrollmyndigheterna beviljas tillgång till de data som behövs för att bedöma utformningen, utvecklingen, produktionen och sårbarhetshanteringen av sådana produkter, inbegripet tillhörande intern dokumentation hos respektive ekonomisk aktör.

Artikel 43

Förfarande på nationell nivå för produkter med digitala element som utgör en betydande cybersäkerhetsrisk

1. Om marknadskontrollmyndigheten i en medlemsstat har tillräckliga skäl att anse att en produkt med digitala element, inbegripet dess sårbarhetshantering, utgör en betydande cybersäkerhetsrisk, ska den göra en utvärdering av den berörda produkten med digitala element med avseende på dess uppfyllande av alla krav som fastställs i denna förordning. De berörda ekonomiska aktörerna ska när så krävs samarbeta med marknadskontrollmyndigheten.

   Om marknadskontrollsmyndigheten vid utvärderingen konstaterar att en produkt med digitala element inte uppfyller kraven i denna förordning ska den utan dröjsmål ålägga den berörda ekonomiska aktören att vidta alla lämpliga korrigerande åtgärder för att se till att produkten uppfyller dessa krav eller dra tillbaka produkten från marknaden eller återkalla den inom en rimlig tid som de fastställer i förhållande till typen av risk.

   Marknadskontrollmyndigheten ska informera det berörda anmälda organet om detta. Artikel 18 i förordning (EU) 2019/1020 ska tillämpas på de korrigerande åtgärderna.

2. Om marknadskontrollmyndigheten anser att den bristande överensstämmelsen inte bara gäller det nationella territoriet, ska den informera kommissionen och de andra medlemsstaterna om utvärderingsresultaten och om de åtgärder som den har ålagt aktören att vidta.

3. Tillverkaren ska säkerställa att alla lämpliga korrigerande åtgärder vidtas i fråga om alla berörda produkter med digitala element som den har tillhandahållit på unionsmarknaden.

4. Om tillverkaren av en produkt med digitala element inte vidtar lämpliga korrigerande åtgärder inom den period som avses i punkt 1 andra stycket, ska marknadskontrollmyndigheten vidta alla lämpliga provisoriska åtgärder för att förbjuda eller begränsa tillhandahållandet av produkten på sin nationella marknad, dra tillbaka produkten från den marknaden eller återkalla den.

   Myndigheten ska utan dröjsmål informera kommissionen och de andra medlemsstaterna om dessa åtgärder.

5. I den information som avses i punkt 4 ska alla tillgängliga uppgifter ingå, särskilt de uppgifter som krävs för att kunna identifiera den produkt med digitala element som inte uppfyller kraven, dess ursprung, vilken typ av bristande överensstämmelse som görs gällande och den risk produkten utgör, vilken typ av nationell åtgärd som vidtagits och åtgärdens varaktighet samt den berörda aktörens synpunkter.

Marknadskontrollmyndigheten ska särskilt ange om den bristande överensstämmelsen beror på en eller flera av följande orsaker:

(a) Produkten eller de processer som införts av tillverkaren uppfyller inte de väsentliga kraven i bilaga I.

(b) Det finns brister i de harmoniserade standarder, system för cybersäkerhetscertifiering eller de gemensamma specifikationer som avses i artikel 18.

6. Marknadskontrollmyndigheterna i andra medlemsstater än den som inledde förfarandet ska utan dröjsmål informera kommissionen och de andra medlemsstaterna om alla vidtagna åtgärder och eventuella kompletterande uppgifter som de har tillgång till med avseende på den berörda produktens bristande överensstämmelse samt eventuella invändningar mot den anmälda nationella åtgärden.

7. En provisorisk åtgärd som har vidtagits av en medlemsstat ska anses vara berättigad om inte någon medlemsstat eller kommissionen framför invändningar mot åtgärden inom tre månader från mottagandet av den information som avses i punkt 4. Detta påverkar inte den berörda aktörens processuella rättigheter i enlighet med artikel 18 i förordning (EU) 2019/1020.

8. Marknadskontrollmyndigheterna i alla medlemsstater ska säkerställa att lämpliga begränsande åtgärder vidtas utan dröjsmål med avseende på den berörda produkten, till exempel att produkten dras tillbaka från marknaden.

Artikel 44

Unionens förfarande i fråga om skyddsåtgärder

1. Om en medlemsstat inom tre månader efter mottagandet av den anmälan som avses i artikel 43.4 har gjort invändningar mot en åtgärd som vidtagits av en annan medlemsstat, eller om kommissionen anser att åtgärden strider mot unionslagstiftningen, ska kommissionen utan dröjsmål inleda samråd med den berörda medlemsstaten och den eller de ekonomiska aktörerna och ska utvärdera den nationella åtgärden. På grundval av utvärderingsresultaten ska kommissionen besluta om den nationella åtgärden är berättigad eller inte inom nio månader från den anmälan som avses i artikel 43.4 och meddela beslutet till den berörda medlemsstaten.

2. Om den nationella åtgärden anses vara berättigad, ska alla medlemsstater vidta de åtgärder som krävs för att säkerställa att den produkt med digitala element som inte uppfyller kraven dras tillbaka från deras marknader och underrätta kommissionen om detta. Om den nationella åtgärden anses omotiverad ska den medlemsstat som berörs återkalla åtgärden.

3. Om den nationella åtgärden anses vara berättigad och produktens bristande överensstämmelse kan tillskrivas brister i de harmoniserade standarderna ska kommissionen tillämpa det förfarande som föreskrivs i artikel 10 i förordning (EU) nr 1025/2012.

4. Om den nationella åtgärden anses motiverad och produktens bristande överensstämmelse kan tillskrivas brister i ett europeiskt system för cybersäkerhetscertifiering som avses i artikel 18, ska kommissionen överväga att

ändra eller upphäva den genomförandeakt enligt artikel 18.4 som specificerar presumtionen om överensstämmelse för det certifieringssystemet.

5. Om den nationella åtgärden anses motiverad och produktens bristande överensstämmelse kan tillskrivas i de gemensamma specifikationer som avses i artikel 19, ska kommissionen överväga att ändra eller upphäva den genomförandeakt enligt artikel 19 som fastställer dessa gemensamma specifikationer.

Artikel 45

Förfarande på EU-nivå för produkter med digitala element som utgör en betydande cybersäkerhetsrisk

1. Om kommissionen har tillräckliga skäl, däribland baserat på information från Enisa, att anse att en produkt med digitala element som utgör en betydande cybersäkerhetsrisk inte uppfyller kraven enligt denna förordning får den begära att de berörda marknadskontrollmyndigheterna gör en utvärdering av överensstämmelsen och följer de förfaranden som avses i artikel 43.

2. Vid exceptionella omständigheter som motiverar ett omedelbart ingripande för att bevara en välfungerande inre marknad, och där kommissionen har tillräckliga skäl att anse att den produkt som avses i punkt 1 fortfarande inte uppfyller kraven enligt denna förordning och inga effektiva åtgärder har vidtagits av de berörda marknadskontrollmyndigheterna, får kommissionen begära att Enisa gör utvärderingen av överensstämmelsen. Kommissionen ska underrätta de berörda marknadskontrollmyndigheterna om detta. De berörda ekonomiska aktörerna ska samarbeta med Enisa på det sätt som behövs.

3. Baserat på Enisas utvärdering får kommissionen besluta att en korrigerande eller begränsande åtgärd krävs på unionsnivå. Därför ska kommissionen utan dröjsmål samråda med de berörda medlemsstaterna och berörda ekonomiska aktörer (en eller flera).

4. Baserat på det samråd som avses i punkt 3 får kommissionen anta genomförandeakter för att besluta om korrigerande eller begränsande åtgärder på unionsnivå, inbegripet beslut om tillbakadragande från marknaden eller återkallande, inom en rimlig tid i förhållande till typen av risk. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 51.2.

5. Kommissionen ska omedelbart delge berörda ekonomiska aktörer det beslut som avses i punkt 4. Medlemsstaterna ska utan dröjsmål genomföra de akter som avses i punkt 4 och underrätta kommissionen om detta.

6. Punkterna 2–5 är tillämpliga under den tid som den exceptionella situation som motiverade kommissionens ingripande varar och så länge som respektive produkt inte bringas till överensstämmelse med denna förordning.

Artikel 46

Produkter med digitala element som överensstämmer med kraven men utgör en betydande cybersäkerhetsrisk

1. Om en marknadskontrollmyndighet i en medlemsstat, efter att ha gjort en utvärdering enligt artikel 43, konstaterar att en produkt med digitala element och de processer som införts av tillverkaren visserligen uppfyller kraven i denna förordning men ändå utgör en betydande cybersäkerhetsrisk och dessutom utgör en risk för människors

hälsa och säkerhet, för efterlevnad av skyldigheter enligt unionsrätt eller nationell rätt avsedda att skydda de grundläggande rättigheterna, för tillgången till och autenticiteten, integriteten eller konfidentialiteten för tjänster som väsentliga entiteter av den typ som avses i [bilaga I till direktiv XXX / XXXX (NIS2)] erbjuder med användning av ett elektroniskt informationssystem eller för andra aspekter av skyddet av allmänintresset, ska den ålägga den berörda aktören att vidta alla lämpliga åtgärder för att säkerställa att produkten med digitala element och de processer som införts av den berörda tillverkaren inte längre utgör en sådan risk när produkten släpps ut på marknaden, att dra tillbaka produkten med digitala element från marknaden eller att återkalla den inom en rimlig tid i förhållande till typen av risk.

2. Tillverkaren eller andra berörda aktörer ska säkerställa att korrigerande åtgärder vidtas i fråga om berörda produkter med digitala element som de har tillhandahållit på marknaden i unionen inom den tidsfrist som fastställts av den marknadskontrollmyndighet i medlemsstaten som avses i punkt 1.

3. Medlemsstaten ska omedelbart underrätta kommissionen och de andra medlemsstaterna om de åtgärder som vidtagits i enlighet med punkt 1. Informationen ska innehålla alla tillgängliga uppgifter, särskilt de uppgifter som krävs för att kunna identifiera den berörda produkten med digitala element, dess ursprung och leveranskedja, vilken typ av risk som produkten utgör samt vilken typ av nationella åtgärder som vidtagits och deras varaktighet.

4. Kommissionen ska utan dröjsmål inleda samråd med medlemsstaterna och den berörda ekonomiska aktören samt utvärdera de nationella åtgärder som vidtagits. På grundval av utvärderingsresultaten ska kommissionen besluta om åtgärden är berättigad eller inte, och vid behov föreslå lämpliga åtgärder.

5. Kommissionen ska rikta sitt beslut till medlemsstaterna.

6. Om kommissionen har tillräckliga skäl, däribland baserat på information från Enisa, att anse att en produkt med digitala element som uppfyller kraven i denna förordning ändå utgör de risker som avses i punkt 1, får den begära att berörda marknadskontrollmyndigheter (en eller flera) gör en utvärdering av överensstämmelsen och följer de förfaranden som avses i artikel 43 och punkterna 1, 2 och 3 i denna artikel.

7. Vid exceptionella omständigheter som motiverar ett omedelbart ingripande för att bevara en välfungerande inre marknad, och där kommissionen har tillräckliga skäl att anse att den produkt som avses i punkt 6 fortsätter att utgöra de risker som avses i punkt 1 och att inga effektiva åtgärder har vidtagits av de berörda nationella marknadskontrollmyndigheterna, får kommissionen begära att Enisa gör en utvärdering av de risker som produkten utgör och ska underrätta de berörda marknadskontrollmyndigheterna om detta. De berörda ekonomiska aktörerna ska samarbeta med Enisa på det sätt som behövs.

8. Baserat på Enisas utvärdering enligt punkt 7 får kommissionen fastställa att en korrigerande eller begränsande åtgärd krävs på unionsnivå. Då ska den utan dröjsmål samråda med de berörda medlemsstaterna och berörda ekonomiska aktörer (en eller flera).

9. Baserat på det samråd som avses i punkt 8 får kommissionen anta genomförandeakter för att besluta om korrigerande eller begränsande åtgärder på unionsnivå, inbegripet beslut om tillbakadragande från marknaden eller återkallande,

inom en rimlig tid i förhållande till typen av risk. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 51.2.

10. Kommissionen ska omedelbart delge berörda aktörer det beslut som avses i punkt 9. Medlemsstaterna ska genomföra dessa akter utan dröjsmål och underrätta kommissionen om detta.

11. Punkterna 6–10 ska tillämpas under den tid som den exceptionella situation som motiverade kommissionens ingripande varar och så länge som respektive produkt fortsätter att utgöra de risker som avses i punkt 1.

Artikel 47

Formell bristande överensstämmelse

1. Om marknadskontrollmyndigheten i en medlemsstat konstaterar något av följande ska den ålägga den berörda tillverkaren att åtgärda den bristande överensstämmelsen:

   (a) Märkningen om överensstämmelse har anbringats i strid med artiklarna 21 och 22.

   (b) Märkning om överensstämmelse saknas.

   (c) Det har inte upprättats någon EU-försäkran om överensstämmelse.

   (d) EU-försäkran om överensstämmelse har inte upprättats på ett korrekt sätt.

   (e) Identifikationsnumret för det anmälda organ som deltar i förfarandet för bedömning av överensstämmelse har i förekommande fall inte anbringats.

   (f) Den tekniska dokumentationen är antingen inte tillgänglig eller inte komplett.

2. Om sådan bristande överensstämmelse som avses i punkt 1 kvarstår ska den berörda medlemsstaten vidta lämpliga åtgärder för att begränsa eller förbjuda tillhandahållandet av produkten med digitala element på marknaden eller säkerställa att den återkallas eller dras tillbaka från marknaden.

Artikel 48

Marknadskontrollmyndigheternas gemensamma aktiviteter

1. Marknadskontrollmyndigheter får komma överens med andra berörda myndigheter om att genomföra gemensamma aktiviteter för att säkerställa cybersäkerheten och skyddet av konsumenter med avseende på specifika produkter med digitala element som släpps ut eller tillhandahålls på marknaden, i synnerhet produkter som ofta befinns utgöra cybersäkerhetsrisker.

2. Kommissionen eller Enisa får föreslå gemensamma aktiviteter för att kontrollera överensstämmelsen med denna förordning vilka ska genomföras av marknadskontrollmyndigheter baserat på indikationer eller information om potentiell bristande överensstämmelse i flera medlemsstater med kraven i denna förordning när det gäller produkter som omfattas av denna förordning.

3. Marknadskontrollmyndigheterna och i tillämpliga fall kommissionen ska säkerställa att överenskommelsen om att genomföra gemensamma aktiviteter inte leder till illojal konkurrens mellan ekonomiska aktörer och inte har någon negativ påverkan på objektiviteten, oberoendet och opartiskheten för parterna i överenskommelsen.

4. En marknadskontrollmyndighet får använda all information som framkommer genom de aktiviteter som utförs som ett led i utredningar som den gör.

5. Den berörda marknadskontrollmyndigheten och i tillämpliga fall kommissionen ska göra överenskommelsen om gemensamma aktiviteter, inklusive namnen på de berörda parterna, tillgänglig för allmänheten.

Artikel 49

Samordnade tillsynsåtgärder (sweeps)

1. Marknadskontrollmyndigheterna får besluta att genomföra samtidiga samordnade kontrollåtgärder för specifika produkter med digitala element eller kategorier av sådana produkter för att kontrollera överensstämmelsen med eller upptäcka överträdelser av denna förordning.

2. Om inte annat överenskommits mellan de berörda marknadskontrollmyndigheterna ska samordnade tillsynsåtgärder samordnas av kommissionen. Samordnaren av de samordnade tillsynsåtgärderna får, när så är lämpligt, offentliggöra de sammanställda resultaten.

3. Enisa får vid utförandet av sina uppgifter, däribland baserat på de anmälningar som inkommit i enlighet med artikel 11.1 och 11.2, identifiera produktkategorier som får omfattas av samordnade tillsynsåtgärder. Förslaget om samordnade tillsynsåtgärder ska lämnas till den potentiella samordnare som avses i punkt 2 för att övervägas av marknadskontrollmyndigheterna.

4. I samband med samordnade tillsynsåtgärder får marknadskontrollmyndigheterna utnyttja de utredningsbefogenheter som fastställs i artiklarna 41–47 och andra befogenheter som tilldelats dem enligt nationell rätt.

5. Marknadskontrollmyndigheterna får bjuda in kommissionens tjänstemän och andra medföljande personer som bemyndigats av kommissionen att delta i samordnade tillsynsåtgärder.

KAPITEL VI

DELEGERADE BEFOGENHETER OCH KOMMITTÉFÖRFARANDE

Artikel 50

Utövande av delegeringen

1. Befogenheten att anta delegerade akter ges till kommissionen med förbehåll för de villkor som anges i denna artikel.

2. Den befogenhet att anta delegerade akter som avses i artiklarna 2.4, 6.2, 6.3, 6.5, 20.5 och 23.5 ska ges till kommissionen.

3. Den delegering av befogenhet som avses i artiklarna 2.4, 6.2, 6.3, 6.5, 20.5 och 23.5 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.

4. Innan kommissionen antar en delegerad akt ska den samråda med experter som utsetts av varje medlemsstat i enlighet med principerna i det interinstitutionella avtalet av den 13 april 2016 om bättre lagstiftning.

5. Så snart kommissionen antar en delegerad akt ska den samtidigt delge Europaparlamentet och rådet denna.

6. En delegerad akt som antas enligt artiklarna 2.4, 6.2, 6.3, 6.5, 20.5 och 23.5 ska träda i kraft endast om varken Europaparlamentet eller rådet har gjort invändningar mot den delegerade akten inom en period på 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.

Artikel 51

Kommittéförfarande

1. Kommissionen ska biträdas av en kommitté. Denna kommitté ska vara en kommitté i den mening som avses i förordning (EU) nr 182/2011.

2. När det hänvisas till denna punkt ska artikel 5 i förordning (EU) nr 182/2011 tillämpas.

3. Om kommitténs yttrande ska inhämtas genom skriftligt förfarande, ska det förfarandet avslutas utan resultat om kommitténs ordförande, inom tidsfristen för att avge yttrandet, så beslutar eller en kommittéledamot så begär.

KAPITEL VII

KONFIDENTIALITET OCH SANKTIONER

Artikel 52

Konfidentialitet

1. Alla parter som deltar i tillämpningen av denna förordning ska respektera konfidentialiteten för den information och de data som de erhåller när de utför sina uppgifter och sin verksamhet på ett sådant sätt att de skyddar följande:

   (a) Immateriella rättigheter och en fysisk eller juridisk persons konfidentiella affärsinformation eller företagshemligheter, inklusive källkod, utom i de fall som avses i artikel 5 i Europaparlamentets och rådets direktiv 2016/943[24].

   (b) Ett effektivt genomförande av denna förordning, särskilt med avseende på inspektioner, utredningar eller revisioner.

   (c) Intressen som rör allmän och nationell säkerhet.

   (d) Integriteten i straffrättsliga eller administrativa förfaranden.

[24] Europaparlamentets och rådets direktiv (EU) 2016/943 av den 8 juni 2016 om skydd mot att icke röjd know-how och företagsinformation (företagshemligheter) olagligen anskaffas, utnyttjas och röjs (EUT L 157, 15.6.2016, s. 1).

2. Utan att det påverkar tillämpningen av punkt 1 får information som utbyts på konfidentiell basis mellan marknadskontrollmyndigheterna och mellan marknadskontrollmyndigheter och kommissionen inte lämnas ut utan föregående samtycke från den marknadskontrollmyndighet som ursprungligen lämnat informationen.

3. Punkterna 1 och 2 påverkar inte kommissionens, medlemsstaternas och de anmälda organens rättigheter och skyldigheter när det gäller att utbyta information och utfärda varningar och inte heller de berörda personernas skyldighet att lämna information enligt medlemsstaternas straffrätt.

4. Kommissionen och medlemsstaterna får vid behov utbyta känslig information med berörda myndigheter i tredjeländer med vilka de har slutit bilaterala eller multilaterala avtal om konfidentialitet som garanterar en tillräcklig skyddsnivå.

Artikel 53

Sanktioner

1. Medlemsstaterna ska fastställa regler om sanktioner för ekonomiska aktörers överträdelser av bestämmelserna i denna förordning och vidta alla nödvändiga åtgärder för att säkerställa att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande.

2. Medlemsstaterna ska till kommissionen anmäla dessa regler och åtgärder utan dröjsmål samt utan dröjsmål eventuella ändringar som berör dem.

3. Bristande efterlevnad av de väsentliga cybersäkerhetskraven i bilaga I och de skyldigheter som fastställs i artiklarna 10 och 11 ska medföra administrativa sanktionsavgifter på upp till 15 000 000 EUR eller, om överträdelsen begås av ett företag, upp till 2,5 % av dess totala globala årsomsättning under det föregående räkenskapsåret, beroende på vilket som är högst.

4. Bristande efterlevnad av andra bestämmelser i denna förordning ska bli föremål för administrativa sanktionsavgifter på upp till 10 000 000 EUR eller, om överträdelsen begås av ett företag, upp till 2 % av dess totala globala årsomsättning för det föregående räkenskapsåret, beroende på vilket som är högst.

5. Tillhandahållande av oriktig, ofullständig eller vilseledande information till anmälda organ och marknadskontrollmyndigheter som svar på en begäran ska medföra administrativa sanktionsavgifter på upp till 5 000 000 EUR eller, om överträdelsen begås av ett företag, upp till 1 % av dess totala globala årsomsättning för det föregående räkenskapsåret, beroende på vilket som är högst.

6. Vid beslut om storleken på den administrativa sanktionsavgiften i varje enskilt fall ska alla relevanta omständigheter i den specifika situationen beaktas och vederbörlig hänsyn ska tas till

   (a) överträdelsens art, svårighetsgrad och varaktighet samt dess konsekvenser,

   (b) huruvida administrativa sanktionsavgifter redan har påförts av andra marknadskontrollmyndigheter på samma aktör för en liknande överträdelse,

   (c) storleken på och marknadsandelen för den aktör som begått överträdelsen.

7. Marknadskontrollmyndigheter som påför administrativa sanktionsavgifter ska förmedla denna information till marknadskontrollmyndigheterna i andra

medlemsstater via det informations- och kommunikationssystem som avses i artikel 34 i förordning (EU) 2019/1020.

8. Varje medlemsstat ska fastställa regler för huruvida och i vilken utsträckning administrativa sanktionsavgifter kan påföras offentliga myndigheter och organ som är inrättade i medlemsstaten.

9. Beroende på medlemsstatens rättssystem kan reglerna om administrativa sanktionsavgifter tillämpas på ett sådant sätt att sanktionsavgifterna utdöms av behöriga nationella domstolar eller andra organ, i enlighet med befogenheter som fastställs på nationell nivå i dessa medlemsstater. Tillämpningen av sådana regler i dessa medlemsstater ska ha motsvarande verkan.

10. Administrativa sanktionsavgifter får, beroende på omständigheterna i det enskilda fallet, påföras utöver eventuella andra korrigerande eller begränsande åtgärder som marknadskontrollmyndigheterna tillämpar på samma överträdelse.

KAPITEL VIII

ÖVERGÅNGS- OCH SLUTBESTÄMMELSER

Artikel 54

Ändring av förordning (EU) 2019/1020

I bilaga I till förordning (EU) 2019/1020 ska följande punkt läggas till:

”71. [Förordning XXX][cyberresiliensakten]”.

Artikel 55

Övergångsbestämmelser

1. EU-typkontrollintyg och beslut om godkännande som utfärdats avseende cybersäkerhetskrav för produkter med digitala element som omfattas av andra bestämmelser i unionens harmoniseringslagstiftning ska fortsätta gälla till och med den [42 månader efter dagen för denna förordnings ikraftträdande], såvida de inte löper ut före den dagen, eller något annat anges i annan unionslagstiftning, i vilket fall de förblir giltiga i enlighet med den lagstiftningen.

2. Produkter med digitala element som har släppts ut på marknaden före den [tillämpningsdagen för denna förordning enligt artikel 57] ska omfattas av kraven i denna förordning endast om de, från och med den dagen, är föremål för väsentliga ändringar av utformningen eller det avsedda ändamålet.

3. Som avvikelse från punkt 2 ska de skyldigheter som fastställs i artikel 11 tillämpas på alla produkter med digitala element som omfattas av denna förordnings tillämpningsområde och som har släppts ut på marknaden före den [tillämpningsdagen för denna förordning enligt artikel 57].

Artikel 56

Utvärdering och översyn

Kommissionen ska senast [36 månader efter den dag då denna förordning börjar tillämpas] och därefter vart fjärde år, överlämna en rapport om utvärderingen och översynen av denna förordning till Europaparlamentet och rådet. Rapporten ska offentliggöras.

Artikel 57

Ikraftträdande och tillämpning

Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Den ska tillämpas från och med den [24 månader efter dagen för denna förordnings ikraftträdande]. Artikel 11 ska dock tillämpas från och med den [12 månader efter denna förordnings ikraftträdande].

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den

På Europaparlamentets vägnar	*På rådets vägnar*
The President	*Ordförande*

FINANSIERINGSÖVERSIKT FÖR RÄTTSAKT

1. GRUNDLÄGGANDE UPPGIFTER OM FÖRSLAGET ELLER INITIATIVET

1.1. Förslagets eller initiativets titel

1.2. Berörda politikområden

1.3. Förslaget eller initiativet avser

1.4. Mål

1.4.1. Allmänt/allmänna mål:

1.4.2. Specifikt/specifika mål:

1.4.3. Verkan eller resultat som förväntas

1.4.4. Prestationsindikatorer

1.5. Grunder för förslaget eller initiativet

1.5.1. Krav som ska uppfyllas på kort eller lång sikt, inbegripet en detaljerad tidsplan för genomförandet av initiativet

1.5.2. Mervärdet av en åtgärd på unionsnivå (som kan följa av flera faktorer, t.ex. samordningsfördelar, rättssäkerhet, ökad effektivitet eller komplementaritet). Med ”mervärdet i unionens intervention” i denna punkt avses det värde en åtgärd från unionens sida tillför utöver det värde som annars skulle ha skapats av enbart medlemsstaterna.

1.5.3. Erfarenheter från tidigare liknande åtgärder

1.5.4. Förenlighet med den fleråriga budgetramen och eventuella synergieffekter med andra relevanta instrument

1.5.5. En bedömning av de olika finansieringsalternativ som finns att tillgå, inbegripet möjligheter till omfördelning

1.6. Beräknad varaktighet för och beräknade budgetkonsekvenser av förslaget eller initiativet

1.7. Planerad metod för genomförandet

2. FÖRVALTNING

2.1. Regler om uppföljning och rapportering

2.2. Förvaltnings- och kontrollsystem

2.2.1. Motivering av den genomförandemetod, de finansieringsmekanismer, de betalningsvillkor och den kontrollstrategi som föreslås

2.2.2. Uppgifter om identifierade risker och om det eller de interna kontrollsystem som inrättats för att begränsa riskerna

2.2.3. Beräkning och motivering av kontrollernas kostnadseffektivitet (dvs. förhållandet mellan kostnaden för kontrollerna och värdet av de medel som förvaltas) och en bedömning av den förväntade risken för fel (vid betalning och vid avslutande)

2.3. Åtgärder för att förebygga bedrägeri och oriktigheter

3. BERÄKNADE BUDGETKONSEKVENSER AV FÖRSLAGET ELLER INITIATIVET

3.1. Berörda rubriker i den fleråriga budgetramen och budgetrubriker i den årliga budgetens utgiftsdel

3.2. Förslagets beräknade budgetkonsekvenser på anslagen

3.2.1. Sammanfattning av beräknad inverkan på driftsanslagen

3.2.2. Beräknad output som finansieras med driftsanslag

3.2.3. Sammanfattning av beräknad inverkan på de administrativa anslagen

3.2.4. Förenlighet med den gällande fleråriga budgetramen

3.2.5. Bidrag från tredje part

3.3. Beräknad inverkan på inkomsterna

FINANSIERINGSÖVERSIKT FÖR RÄTTSAKT

1. GRUNDLÄGGANDE UPPGIFTER OM FÖRSLAGET ELLER INITIATIVET

1.1. Förslagets eller initiativets titel

Förslag till förordning om övergripande cybersäkerhetskrav för produkter med digitala element (cyberresiliensakten)

1.2. Berörda politikområden

Kommunikationsnät, innehåll och teknik

1.3. Förslaget eller initiativet avser

× **en ny åtgärd**

☐ **en ny åtgärd som bygger på ett pilotprojekt eller en förberedande åtgärd**[37]

☐ **en förlängning av en befintlig åtgärd**

☐ **en sammanslagning eller omdirigering av en eller flera åtgärder mot en annan/en ny åtgärd**

1.4. Mål

1.4.1. Allmänt/allmänna mål:

Förslaget har två huvudmål som syftar till att säkerställa en korrekt fungerande inre marknad: 1) **Skapa förutsättningar för utvecklingen av säkra produkter med digitala element** genom att säkerställa att hårdvaru- och programvaruprodukter har färre sårbarheter när de släpps ut på marknaden och att tillverkarna tar säkerheten på allvar under hela produktens livscykel. 2) **Skapa förutsättningar för att användarna ska kunna ta hänsyn till cybersäkerheten när de väljer och använder produkter med digitala element**.

1.4.2. Specifikt/specifika mål:

Fyra specifika mål fastställdes i förslaget: i) Att säkerställa att tillverkarna förbättrar säkerheten för produkter med digitala element från utformnings- och utvecklingsfasen och under hela produktens livscykel. ii) Att säkerställa en sammanhängande cybersäkerhetsram, som främjar överensstämmelse för hårdvaru- och programvaruproducenter. iii) Att förbättra transparensen för säkerhetsegenskaperna hos produkter med digitala element. iv) Att möjliggöra en säker användning av produkter med digitala element för företag och konsumenter.

Verkan eller resultat som förväntas

Beskriv den verkan som förslaget eller initiativet förväntas få på de mottagare eller den del av befolkningen som berörs.

Förslaget skulle ge betydande fördelar för de olika intressenterna. För företagen skulle det förhindra att olikartade säkerhetsregler gäller för produkter med digitala element, och det skulle sänka kostnaderna för uppfyllande av kraven i cybersäkerhetslagstiftningen. Det skulle minska antalet cyberincidenter, kostnaden

[37] I den mening som avses i artikel 58.2 a eller b i budgetförordningen.

för incidenthantering och risken för skadat anseende. För EU som helhet beräknas att initiativet kan minska kostnaderna från incidenter som påverkar företag med omkring 180–290 miljarder EUR per år[38]. Det skulle leda till ökad omsättning tack vare en ökad efterfrågan på produkter med digitala element. Det skulle förbättra företagens globala anseende och leda till en ökad efterfrågan också utanför EU. För användarna skulle det rekommenderade alternativet öka transparensen för säkerhetsegenskaper och underlätta användningen av produkter med digitala element. Konsumenter och medborgare skulle också gagnas av ett bättre skydd för sina grundläggande rättigheter, såsom personlig integritet och skydd av personuppgifter.

Samtidigt skulle förslaget medföra kostnader för överensstämmelse och kontroll av efterlevnad för företag, anmälda organ och offentliga myndigheter, inbegripet ackrediterings- och marknadskontrollmyndigheter. För programvaruutvecklare och hårdvarutillverkare kommer det att medföra direkta efterlevnadskostnader för nya säkerhetskrav, bedömning av överensstämmelse, dokumentation och rapporteringsskyldigheter, uppgående till sammanlagt omkring 29 miljarder EUR för ett beräknat marknadsvärde på 1 485 miljarder EUR i omsättning[39]. Användare, såsom företagsanvändare, konsumenter och medborgare, kan drabbas av högre priser på produkter med digitala element. Detta bör dock ses mot bakgrund av de betydande fördelar som beskrivs ovan.

1.4.3. Prestationsindikatorer

Ange indikatorer för övervakning av framsteg och resultat.

För att testa om tillverkare förbättrar säkerheten för sina produkter med digitala element efter utformnings- och utvecklingsfasen och under hela produkternas livscykel kan flera indikatorer beaktas. Det kan handla om antalet betydande incidenter i unionen som orsakats av sårbarheter, andelen hårdvaru- och programvarutillverkare som följer en systematisk säker utvecklingslivscykel, en kvalitativ analys av säkerheten hos produkter med digitala element, en kvantitativ och kvalitativ bedömning av sårbarhetsdatabaser, hur ofta tillverkare tillhandahåller säkerhetsprogramfixar eller det genomsnittliga antalet dagar mellan upptäckten av en sårbarhet och tillhandahållandet av säkerhetsprogramfixar.

En indikator på en sammanhängande cybersäkerhetsram kan vara avsaknaden av riktad produktspecifik nationell cybersäkerhetslagstiftning.

En indikator på ökad transparens i fråga om säkerhetsegenskaperna hos produkter med digitala element kan vara andelen produkter med digitala element som levereras med information om säkerhetsegenskaper. Andelen produkter med digitala element som levereras med instruktioner till användaren om en säker användning kan också användas som en indikator på om organisationer och konsumenter har möjlighet att använda de berörda produkterna på ett säkert sätt.

När det gäller övervakningen av förordningens effekter kan vissa indikatorer övervägas för detta syfte, vilket ska bedömas av kommissionen, vid behov med stöd från Enisa. Beroende på de operativa syften som ska uppnås anges nedan några

[38] Se [Arbetsdokument från kommissionens avdelningar om konsekvensbedömningsrapporten som åtföljer förordningen om övergripande cybersäkerhetskrav för produkter med digitala element].

[39] Se [Arbetsdokument från kommissionens avdelningar om konsekvensbedömningsrapporten som åtföljer förordningen om övergripande cybersäkerhetskrav för produkter med digitala element].

exempel på övervakningsindikatorer som skulle kunna användas för att bedöma hur väl de övergripande cybersäkerhetskraven fungerar:

För bedömning av cybersäkerhetsnivån för produkter med digitala element:

- Statistik och kvalitativ analys av incidenter som påverkar produkter med digitala element samt hur incidenterna har hanterats. Dessa uppgifter kan samlas in och bedömas av kommissionen med stöd av Enisa.

- Kända sårbarheter som registrerats samt analys av hanteringen av dessa. En sådan analys kan göras av Enisa, baserat på den europeiska sårbarhetsdatabas som inrättats på grundval av [direktiv XXX/ XXXX (NIS2)].

- Enkäter till hårdvaru- och programvarutillverkare för att följa upp utvecklingen.

För bedömning av nivån av information om säkerhetsegenskaper, säkerhetsstöd, uttjänta produkter och aktsamhetskrav: Resultat av enkäter bland användare och företag som genomförs av kommissionen med stöd av Enisa.

För bedömning av genomförandet är kommissionens strävan att säkerställa att bedömningar av överensstämmelse utförs på ett effektivt sätt. Därför kommer en standardiseringsbegäran att utfärdas och dess genomförande att följas. Kommissionen kommer också att kontrollera de anmälda organens kapacitet och, i förekommande fall, certifieringsorganens.

När det gäller tillämpningen: På grundval av medlemsstaternas rapporter kommer kommissionen att kontrollera att nationella initiativ inte rör aspekter som omfattas av förordningen.

1.5. Grunder för förslaget eller initiativet

1.5.1. Krav som ska uppfyllas på kort eller lång sikt, inbegripet en detaljerad tidsplan för genomförandet av initiativet

Förordningen bör vara helt tillämplig 24 månader efter ikraftträdandet. Delar av styrningsstrukturen bör dock ha upprättats dessförinnan. Medlemsstaterna bör särskilt ha utsett befintliga myndigheter och/eller inrättat nya myndigheter till att utföra de uppgifter som fastställs i förordningen.

1.5.2. Mervärdet av en åtgärd på unionsnivå (som kan följa av flera faktorer, t.ex. samordningsfördelar, rättssäkerhet, ökad effektivitet eller komplementaritet). Med ”mervärdet i unionens intervention” i denna punkt avses det värde en åtgärd från unionens sida tillför utöver det värde som annars skulle ha skapats av enbart medlemsstaterna.

Cybersäkerhetens starka gränsöverskridande dimension och det ökande antalet incidenter med spridningseffekter över gränser och mellan sektorer och produkter innebär att målen inte kan uppnås på ett effektivt sätt av medlemsstaterna på egen hand. Eftersom marknaderna för produkter med digitala element är globala möter medlemsstaterna på sina territorier samma risker för samma produkter med digitala element. En framväxande fragmenterad ram bestående av potentiellt olika nationella regler riskerar att stå i vägen för en öppen och konkurrenspräglad inre marknad för produkter med digitala element. Det krävs alltså gemensamma åtgärder på EU-nivå för att öka förtroendet hos användarna och stärka dragningskraften för EU-produkter med digitala element. Det skulle också gagna den digitala inre marknaden genom att

skapa rättssäkerhet och lika spelregler för alla försäljare av produkter med digitala element.

1.5.3. Erfarenheter från tidigare liknande åtgärder

Cyberresiliensakten är den första förordningen av sitt slag, som inför cybersäkerhetskrav för utsläppandet på marknaden av produkter med digitala element. Den bygger dock på den nya lagstiftningsramen och lärdomarna från genomförandet av unionens befintliga harmoniseringslagstiftning för en mängd produkter, i synnerhet vad gäller förberedelserna av genomförandet inbegripet sådana aspekter som utarbetandet av harmoniserade standarder.

1.5.4. Förenlighet med den fleråriga budgetramen och eventuella synergieffekter med andra relevanta instrument

Genom förordningen om övergripande cybersäkerhetskrav för produkter med digitala element fastställs nya cybersäkerhetskrav för alla produkter med digitala element som släpps ut på EU-marknaden, vilket är betydligt mer långtgående än kraven i befintlig lagstiftning. Samtidigt bygger förslaget på den nya lagstiftningsramens befintliga struktur. Det bygger alltså vidare på befintliga strukturer och förfaranden inom den ramen, såsom samarbete mellan anmälda organ och marknadskontroll, moduler för bedömning av överensstämmelse och utveckling och utveckling av harmoniserade standarder. Det nya förslaget bygger också på vissa strukturer som utvecklats i enlighet med annan cybersäkerhetslagstiftning såsom direktiv 2016/1148 (NIS-direktivet), [direktiv XXX/ XXXX (NIS2)] och förordning 2019/881 (cybersäkerhetsakten).

1.5.5. En bedömning av de olika finansieringsalternativ som finns att tillgå, inbegripet möjligheter till omfördelning

Förvaltningen av de verksamhetsområden som Enisa får ansvaret för är anpassade till Enisas befintliga mandat och allmänna uppgifter. Dessa verksamhetsområden kan kräva särskilda profiler eller nya uppdrag, men de skulle inte vara omfattande utan kan absorberas av Enisas befintliga resurser och lösas genom omfördelning eller sammankoppling av olika uppdrag. Ett av de viktigaste verksamhetsområdena som tilldelas Enisa rör insamlingen och behandlingen av tillverkarnas anmälningar av utnyttjade produktsårbarheter. [Direktiv XXX/ XXXX (NIS2)] har redan gett Enisa i uppdrag att inrätta en europeisk sårbarhetsdatabas där allmänt kända sårbarheter kan meddelas och registreras på frivillig grund, för att användarna ska kunna vidta lämpliga riskreducerande åtgärder. De resurser som avsatts för detta skulle också kunna användas för de nya ovannämnda uppgifterna avseende anmälningar av produktsårbarheter. Det skulle kunna säkerställa en effektiv användning av befintliga resurser och även skapa nödvändiga synergier mellan sådana uppdrag som kan förbättra underlaget för Enisas analyser av cybersäkerhetsrisker och hot.

1.6. Beräknad varaktighet för och beräknade budgetkonsekvenser av förslaget eller initiativet

☐ **begränsad varaktighet**

– ☐ verkan från och med [den DD/MM]ÅÅÅÅ till och med [den DD/MM]ÅÅÅÅ

– ☐ budgetkonsekvenser från och med YYYY till och med YYYY för åtagandebemyndiganden och från och med YYYY till och med YYYY för betalningsbemyndiganden.

× **obegränsad varaktighet**

– Efter en inledande period från 2025,

– beräknas genomförandetakten nå en stabil nivå.

1.7. Planerad metod för genomförandet[40]

☐ **Direkt förvaltning** som sköts av kommissionen

– × av dess avdelningar, vilket också inbegriper personalen vid unionens delegationer;

– ☐ av genomförandeorgan

☐ **Delad förvaltning** med medlemsstaterna

☐ **Indirekt förvaltning** genom att uppgifter som ingår i budgetgenomförandet anförtros

– ☐ tredjeländer eller organ som de har utsett

– ☐ internationella organisationer och organ kopplade till dem (ange vilka)

– ☐ EIB och Europeiska investeringsfonden

– ☐ organ som avses i artiklarna 70 och 71 i budgetförordningen

– ☐ offentligrättsliga organ

– ☐ privaträttsliga organ som har anförtrotts offentliga förvaltningsuppgifter i den utsträckning som de lämnar tillräckliga ekonomiska garantier

– ☐ organ som omfattas av privaträtten i en medlemsstat, som anförtrotts genomförandeuppgifter inom ramen för ett offentlig-privat partnerskap och som lämnar tillräckliga ekonomiska garantier

– ☐ personer som anförtrotts genomförandet av särskilda åtgärder inom Gusp enligt avdelning V i fördraget om Europeiska unionen och som fastställs i den relevanta grundläggande rättsakten

– *Vid fler än en metod, ange kompletterande uppgifter under ”Anmärkningar”.*

Anmärkningar

Genom denna förordning tilldelas Enisa vissa uppgifter, i linje med Enisas befintliga mandat och i synnerhet artikel 3.2 i förordning 2019/881, där det fastställs att Enisa ska utföra de uppgifter som den tilldelas genom unionsrättsakter som fastställer åtgärder för tillnärmning av

[40] Närmare förklaringar av de olika metoderna för genomförande med hänvisningar till respektive bestämmelser i budgetförordningen återfinns på BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx

medlemsstatens lagar och andra författningar som rör cybersäkerhet. I synnerhet får Enisa i uppgift att ta emot anmälningar från tillverkare om aktivt utnyttjade sårbarheter i produkter med digitala element samt om incidenter som påverkar säkerheten för dessa produkter. Enisa bör också vidarebefordra dessa anmälningar till de berörda CSIRT-enheterna och till medlemsstaternas berörda gemensamma kontaktpunkter som utsetts i enlighet med artikel [artikel X] i direktiv [direktiv XXX / XXXX (NIS2)] samt underrätta marknadskontrollmyndigheterna. På grundval av sin insamlade information bör Enisa vartannat år utarbeta en teknisk rapport om nya trender i fråga om cybersäkerhetsrisker i produkter med digitala element, och lämna den till samarbetsgruppen för nät- och informationssäkerhet. Mot bakgrund av Enisas expertis, insamlade information och hotanalyser kan Enisa stödja genomförandeprocessen för denna förordning genom att föreslå gemensamma åtgärder att vidtas av de nationella marknadskontrollmyndigheterna i flera medlemsstater på grundval av indikationer eller information om potentiell bristande överensstämmelse med denna förordning för produkter med digitala element eller identifiera produktkategorier där samtidiga samordnade kontrollåtgärder får organiseras. Kommissionen kan begära att Enisa vid exceptionella omständigheter gör utvärderingar av specifika produkter med digitala element som utgör en betydande cybersäkerhetsrisk, när ett omedelbart ingripande krävs för att bevara en väl fungerande inre marknad.

Alla dessa uppgifter beräknas till omkring 4,5 heltidsekvivalenter från Enisas befintliga resurser och bygger på expertis och förberedande arbete som redan görs av Enisa, bland annat till stöd för det kommande genomförandet av [direktiv XXX/ XXXX (NIS2)] som föranledde en komplettering av Enisas resurser.

2. FÖRVALTNING

2.1. Regler om uppföljning och rapportering

Ange intervall och andra villkor för sådana åtgärder:

Kommissionen kommer, senast 36 månader efter tillämpningsdagen för denna förordning och därefter vart fjärde år, att överlämna en rapport om utvärderingen och översynen av den till Europaparlamentet och rådet. Rapporten ska offentliggöras.

2.2. Förvaltnings- och kontrollsystem

2.2.1. Motivering av den genomförandemetod, de finansieringsmekanismer, de betalningsvillkor och den kontrollstrategi som föreslås

Genom denna förordning fastställs en ny policy för harmoniserade cybersäkerhetskrav för produkter med digitala element som släpps ut på den inre marknaden under hela produkternas livscykel. Rättsakten kommer att följas av begäranden från kommissionen till europeiska standardiseringsorgan om utveckling av standarder.

För att klara av dessa nya uppgifter är det nödvändigt att på lämpligt sätt förse kommissionens avdelningar med resurser. Kontrollen av efterlevnaden av den nya förordningen beräknas kräva 7 heltidsekvivalenter (varav en nationell expert) för att göra följande:

– Utarbeta en standardiseringsbegäran och/eller gemensamma specifikationer genom genomförandeakter om standardiseringsprocessen inte genomförs med framgång.

– Utarbeta en delegerad akt [inom 12 månader från förordningens ikraftträdande] som specificerar definitionerna av kritiska produkter med digitala element.

– Eventuellt utarbeta delegerade akter för att uppdatera förteckningen över kritiska produkter i klass I och II, specificera om det är nödvändigt med en begränsning eller ett uteslutande av produkter med digitala element som omfattas av andra unionsregler som omfattar krav som ger samma skyddsnivå som denna förordning, införa ett krav på certifiering av vissa mycket kritiska produkter med digitala element baserat på kriterier som fastställs i denna förordning, specificera minimiinnehållet i EU-försäkran om överensstämmelse och komplettera de aspekter som ska ingå i den tekniska dokumentationen.

– Eventuellt utarbeta genomförandeakter avseende formatet för eller innehållet i rapporteringsskyldigheterna, programvaruförteckningen, gemensamma specifikationer eller anbringande av CE-märkning.

– Eventuellt förbereda ett omedelbart ingripande för att införa korrigerande eller begränsande åtgärder vid exceptionella omständigheter för att bevara en välfungerande inre marknad, inbegripet utarbetandet av en genomförandeakt.

– Organisera och samordna medlemsstaternas anmälningar av anmälda organ och samordning av de anmälda organen.

– Stödja samarbetet mellan medlemsstaternas marknadskontrollmyndigheter.

2.2.2. Uppgifter om identifierade risker och om det eller de interna kontrollsystem som inrättats för att begränsa riskerna

För att säkerställa att anmälda organ och marknadskontrollmyndigheter utbyter information och samarbetar väl ansvarar kommissionen för deras samordning. En expertgrupp kommer att inrättas för teknisk expertis och marknadsexpertis.

2.2.3. Beräkning och motivering av kontrollernas kostnadseffektivitet (dvs. förhållandet mellan kostnaden för kontrollerna och värdet av de medel som förvaltas) och en bedömning av den förväntade risken för fel (vid betalning och vid avslutande)

2.3. Med tanke på det låga värdet per transaktion (t.ex. ersättning av resekostnader för en delegat för ett möte) förefaller standardkontrollförfarandena vara tillräckliga när det gäller möteskostnaderna. Åtgärder för att förebygga bedrägeri och oriktigheter

Beskriv förebyggande åtgärder (befintliga eller planerade), t.ex. från strategi för bedrägeribekämpning.

De befintliga bedrägeriförebyggande åtgärder som är tillämpliga på kommissionen kommer att täcka de ytterligare anslag som krävs för denna förordning.

3. BERÄKNADE BUDGETKONSEKVENSER AV FÖRSLAGET ELLER INITIATIVET

3.1. Berörda rubriker i den fleråriga budgetramen och budgetrubriker i den årliga budgetens utgiftsdel

- Befintliga budgetrubriker (även kallade ”budgetposter”)

Schema

- Nya budgetrubriker som föreslås

Ej tillämpligt

3.2. Förslagets beräknade budgetkonsekvenser på anslagen

3.2.1. Sammanfattning av beräknad inverkan på driftsanslagen

– ☑ Förslaget/initiativet kräver inte att driftsanslag tas i anspråk

– ☐ Förslaget/initiativet kräver att driftsanslag tas i anspråk enligt följande:

Miljoner euro (avrundat till tre decimaler)

Rubrik i den fleråriga budgetramen	Nummer	

GD: <…….>			År **N**[41]	År **N+1**	År **N+2**	År **N+3**	För in så många år som behövs för att redovisa varaktigheten för inverkan på resursanvändningen (jfr punkt 1.6)			**TOTALT**
• Driftsanslag										
Budgetrubrik[42]	Åtaganden	(1a)								
	Betalningar	(2 a)								
Budgetrubrik	Åtaganden	(1b)								
	Betalningar	(2b)								
Anslag av administrativ natur som finansieras genom ramanslagen för vissa operativa program[43]										
Budgetrubrik		(3)								
TOTALA anslag	Åtaganden	=1a+1b +3								

41 Med år n avses det år då förslaget eller initiativet ska börja genomföras. Ersätt ”n” med det förväntade första genomförandeåret (till exempel 2021). Detsamma för följande år.

42 Enligt den officiella kontoplanen.

43 Detta avser tekniskt eller administrativt stöd för genomförandet av vissa av Europeiska unionens program och åtgärder (tidigare s.k. BA-poster) samt indirekta och direkta forskningsåtgärder.

för GD <…….>	Betalningar	=2a+2b +3								

• TOTALA driftsanslag	Åtaganden	(4)								
	Betalningar	(5)								
• TOTALA anslag av administrativ natur som finansieras genom ramanslagen för vissa operativa program		(6)								
TOTALA anslag för RUBRIK<….> i den fleråriga budgetramen	Åtaganden	=4+ 6								
	Betalningar	=5+ 6								

Upprepa avsnittet ovan om flera rubriker avseende driftsanslag i budgetramen påverkas av förslaget eller initiativet:

• TOTALA driftsanslag (alla rubriker avseende driftsanslag)	Åtaganden	(4)								
	Betalningar	(5)								
TOTALA anslag av administrativ natur som finansieras genom ramanslagen för vissa operativa program (alla driftsrelaterade rubriker)		(6)								
TOTALA anslag under RUBRIKERNA 1–6 i den fleråriga budgetramen (referensbelopp)	Åtaganden	=4+ 6								
	Betalningar	=5+ 6								

Rubrik i den fleråriga budgetramen	**7**	”Administrativa utgifter”

Detta avsnitt ska fyllas i med hjälp av det datablad för budgetuppgifter av administrativ natur som först ska föras in i bilagan till finansieringsöversikt för rättsakt (bilaga V till de interna bestämmelserna), vilken ska laddas upp i DECIDE som underlag för samråden mellan kommissionens avdelningar.

Miljoner euro (avrundat till tre decimaler)

		År **2024**	År **2025**	År **2026**	År **2027**	**TOTALT**
GD: CNECT						
• Personalresurser		1.030	1.030	1.030	1.030	**4.120**
• Övriga administrativa utgifter		**0.222**	**0.222**	**0.222**	**0.222**	**0.888**
TOTALT GD CNECT	Anslag	**1.252**	**1.252**	**1.252**	**1.252**	**5.008**

TOTALA anslag för RUBRIK 7 i den fleråriga budgetramen	(summa åtaganden = summa betalningar)	**1.252**	**1.252**	**1.252**	**1.252**	**5.008**

Miljoner euro (avrundat till tre decimaler)

		År **2024**	År **2025**	År **2026**	År **2027**	**TOTALT**
TOTALA anslag under RUBRIKERNA 1–7 i den fleråriga budgetramen	Åtaganden	**1.252**	**1.252**	**1.252**	**1.252**	**5.008**
	Betalningar	**1.252**	**1.252**	**1.252**	**1.252**	**5.008**

3.2.2. Beräknad output som finansieras med driftsanslag

Åtagandebemyndiganden i miljoner euro (avrundat till tre decimaler)

Mål- och resultatbeteckning ⇩			År **N**		År **N+1**		År **N+2**		År **N+3**		För in så många år som behövs för att redovisa varaktigheten för inverkan på resursanvändningen (jfr punkt 1.6)						**TOTALT**	
	OUTPUT																	
	Typ[44]	Genomsnittliga kostnader	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Totalt antal	Total kostnad
SPECIFIKT MÅL nr 1[45]…																		
- Output																		
- Output																		
- Output																		
Delsumma för specifikt mål nr 1																		
SPECIFIKT MÅL nr 2…																		
- Output																		
Delsumma för specifikt mål nr 2																		
TOTALT																		

[44] Output som ska anges är de produkter eller tjänster som levererats (t.ex. antal studentutbyten som har finansierats eller antal kilometer väg som har byggts).

[45] Mål som redovisats under punkt 1.4.2: ”Specifikt/specifika mål…”.

3.2.3. Sammanfattning av beräknad inverkan på de administrativa anslagen

– ☐ Förslaget/initiativet kräver inte att anslag av administrativ natur tas i anspråk

– ☑ Förslaget/initiativet kräver att anslag av administrativ natur tas i anspråk enligt följande:

Miljoner euro (avrundat till tre decimaler)

	År **2024**	År **2025**	År **2026**	År **2027**	
RUBRIK 7 i den fleråriga budgetramen					
Personalresurser	1.030	1.030	1.030	1.030	**4.120**
Övriga administrativa utgifter	0.222	0.222	0.222	0.222	**0.888**
Delsumma för RUBRIK 7 i den fleråriga budgetramen	1.252	1.252	1.252	1.252	**5.008**

Utanför RUBRIK 7[46] **i den fleråriga budgetramen**					
Personalresurser					
Andra administrativa kostnader					
Delsumma utanför RUBRIK 7 i den fleråriga budgetramen					

TOTALT	1.252	1.252	1.252	1.252	**5.008**

Personalbehov och andra administrativa kostnader ska täckas genom anslag inom generaldirektoratet vilka redan har avdelats för förvaltningen av åtgärden i fråga, eller genom en omfördelning av anslag inom generaldirektoratet, om så krävs kompletterad med ytterligare resurser som kan tilldelas det förvaltande generaldirektoratet som ett led i det årliga förfarandet för tilldelning av anslag och med hänsyn tagen till begränsningar i fråga om budgetmedel.

[46] Detta avser tekniskt eller administrativt stöd för genomförandet av vissa av Europeiska unionens program och åtgärder (tidigare s.k. BA-poster) samt indirekta och direkta forskningsåtgärder.

3.2.3.1. Beräknat personalbehov

– ☐ Förslaget/initiativet kräver inte att personalresurser tas i anspråk

– ☑ Förslaget/initiativet kräver att personalresurser tas i anspråk enligt följande:

Beräkningarna ska anges i heltidsekvivalenter

		År **2024**	År **2025**	År **2026**	År **2027**
20 01 02 01 (vid huvudkontoret eller vid kommissionens kontor i medlemsstaterna)		6	6	6	6
20 01 02 03 (vid delegationer)					
01 01 01 01 (indirekta forskningsåtgärder)					
01 01 01 11 (direkta forskningsåtgärder)					
Annan budgetrubrik (ange vilken)					
• Extern personal (i heltidsekvivalenter)[47]					
20 02 01 (kontraktsanställda, nationella experter och vikarier finansierade genom ramanslaget)		1	1	1	1
20 02 03 (kontraktsanställda, lokalanställda, nationella experter, vikarier och unga experter som tjänstgör vid delegationerna)					
XX 01 xx **yy zz** [48]	- vid huvudkontoret				
	- vid delegationer				
01 01 01 02 (kontraktsanställda, vikarier och nationella experter som arbetar med indirekta forskningsåtgärder)					
01 01 01 12 (kontraktsanställda, vikarier och nationella experter som arbetar med direkta forskningsåtgärder)					
Annan budgetrubrik (ange vilken)					
TOTALT		**7**	**7**	**7**	**7**

XX motsvarar det politikområde eller den avdelning i budgeten som avses.

Personalbehoven ska täckas med personal inom generaldirektoratet vilka redan har avdelats för förvaltningen av åtgärden i fråga, eller genom en omfördelning av personal inom generaldirektoratet, om så krävs kompletterad med ytterligare resurser som kan tilldelas det förvaltande generaldirektoratet som ett led i det årliga förfarandet för tilldelning av anslag och med hänsyn tagen till begränsningar i fråga om budgetmedel.

Beskrivning av arbetsuppgifter:

Tjänstemän och tillfälligt anställda 6 heltidsekvivalenter x 157 000 €/år = € 942 000	Mål som redovisats under punkt 2.2.1: – Utarbeta en standardiseringsbegäran och/eller gemensamma specifikationer genom genomförandeakter om standardiseringsprocessen inte genomförs med framgång. – Utarbeta en delegerad akt [inom 12 månader från förordningens ikraftträdande] som specificerar definitionerna av kritiska produkter med digitala element. – Eventuellt utarbeta delegerade akter för att uppdatera förteckningen över kritiska produkter i klass I och II, specificera om det är nödvändigt med en begränsning eller ett uteslutande av produkter med digitala element som omfattas av andra unionsregler som omfattar krav som ger samma skyddsnivå som denna förordning, införa ett krav på certifiering av vissa mycket kritiska produkter med digitala element baserat på kriterier som fastställs i denna förordning, specificera minimiinnehållet i EU-försäkran

47 [Denna fotnot förklarar vissa initialförkortningar som inte används i den svenska versionen].

48 Särskilt tak för finansiering av extern personal genom driftsanslag (tidigare s.k. BA-poster).

	om överensstämmelse och komplettera de aspekter som ska ingå i den tekniska dokumentationen. – Eventuellt utarbeta genomförandeakter avseende formatet för eller innehållet i rapporteringsskyldigheterna, programvaruförteckningen, gemensamma specifikationer eller anbringande av CE-märkning. – Eventuellt förbereda ett omedelbart ingripande för att införa korrigerande eller begränsande åtgärder vid exceptionella omständigheter för att bevara en välfungerande inre marknad, inbegripet utarbetandet av en genomförandeakt. – Organisera och samordna medlemsstaternas anmälningar av anmälda organ och samordning av de anmälda organen. – Stödja samarbetet mellan medlemsstaternas marknadskontrollmyndigheter.
Extern personal 1 nationell expert x 88 000 €/år	Mål som redovisats under punkt 2.2.1: – Utarbeta en standardiseringsbegäran och/eller gemensamma specifikationer genom genomförandeakter om standardiseringsprocessen inte genomförs med framgång. – Utarbeta en delegerad akt [inom 12 månader från förordningens ikraftträdande] som specificerar definitionerna av kritiska produkter med digitala element. – Eventuellt utarbeta delegerade akter för att uppdatera förteckningen över kritiska produkter i klass I och II, specificera om det är nödvändigt med en begränsning eller ett uteslutande av produkter med digitala element som omfattas av andra unionsregler som omfattar krav som ger samma skyddsnivå som denna förordning, införa ett krav på certifiering av vissa mycket kritiska produkter med digitala element baserat på kriterier som fastställs i denna förordning, specificera minimiinnehållet i EU-försäkran om överensstämmelse och komplettera de aspekter som ska ingå i den tekniska dokumentationen. – Eventuellt utarbeta genomförandeakter avseende formatet för eller innehållet i rapporteringsskyldigheterna, programvaruförteckningen, gemensamma specifikationer eller anbringande av CE-märkning. – Eventuellt förbereda ett omedelbart ingripande för att införa korrigerande eller begränsande åtgärder vid exceptionella omständigheter för att bevara en välfungerande inre marknad, inbegripet utarbetandet av en genomförandeakt. – Organisera och samordna medlemsstaternas anmälningar av anmälda organ och samordning av de anmälda organen. – Stödja samarbetet mellan medlemsstaternas marknadskontrollmyndigheter.

3.2.4. Förenlighet med den gällande fleråriga budgetramen

Förslaget/initiativet

– x kan finansieras fullständigt genom omfördelningar inom den berörda rubriken i den fleråriga budgetramen.

Ingen omfördelning krävs.

– ☐ kräver användning av den outnyttjade marginalen under den relevanta rubriken i den fleråriga budgetramen och/eller användning av särskilda instrument enligt definitionen i förordningen om den fleråriga budgetramen.

-

– ☐ kräver en översyn av den fleråriga budgetramen.

-

3.2.5. Bidrag från tredje part

Förslaget/initiativet:

– x innehåller inga bestämmelser om samfinansiering från tredje parter

– ☐ innehåller bestämmelser om samfinansiering från tredje parter enligt följande uppskattning:

Anslag i miljoner euro (avrundat till tre decimaler)

	År **N**[49]	År **N+1**	År **N+2**	År **N+3**	För in så många år som behövs för att redovisa varaktigheten för inverkan på resursanvändningen (jfr punkt 1.6)			Totalt
Ange vilket organ som deltar i samfinansieringen								
TOTALA anslag som tillförs genom samfinansiering								

[49] Med år n avses det år då förslaget eller initiativet ska börja genomföras. Ersätt ”n” med det förväntade första genomförandeåret (till exempel 2021). Detsamma för följande år.

3.3. Beräknad inverkan på inkomsterna

– ☐ Förslaget/initiativet påverkar inte budgetens inkomstsida.

– ☐ Förslaget/initiativet påverkar inkomsterna på följande sätt:

– ☐ Påverkan på egna medel

– ☐ Påverkan på andra inkomster

– ange om inkomsterna har avsatts för utgiftsposter☐

Miljoner euro (avrundat till tre decimaler)

Budgetrubrik i den årliga budgetens inkomstdel:	Belopp som förts in för det innevarande budgetåret	Förslagets/initiativets inverkan på inkomsterna[50]						
		År **N**	År **N+1**	År **N+2**	År **N+3**	För in så många år som behövs för att redovisa varaktigheten för inverkan på resursanvändningen (jfr punkt 1.6)		
Artikel …….								

För inkomster avsatta för särskilda ändamål, ange vilka budgetrubriker i utgiftsdelen som berörs.

Övriga anmärkningar (t.ex. vilken metod/formel som har använts för att beräkna inverkan på inkomsterna eller andra relevanta uppgifter).

[50] Vad gäller traditionella egna medel (tullar, sockeravgifter) ska nettobeloppen anges, dvs. bruttobeloppen minus 20 % avdrag för uppbördskostnader.