Regeringskansliet
Faktapromemoria 2022/23:FPM6

Förordning om horisontella cybersäkerhetskrav för produkter med digitala inslag

2022/23:FPM6

Infrastrukturdepartementet

2022-10-31

Dokumentbeteckning

COM(2022) 454 final
Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordning (EU) 2019/1020

Sammanfattning

Den 15 september 2022 presenterade den Europeiska kommissionen (kommissionen) ett förslag till förordning om horisontella cybersäkerhetskrav för produkter med digitala inslag och ändring av förordning 2019/1020 (Cyberresiliensakten).

Syftet med förslaget är att skapa förutsättningar för utveckling av säkra produkter med digitala inslag genom att försäkra att hård- och mjukvara placeras på marknaden med färre sårbarheter och att tillverkare tar större ansvar för produkters cybersäkerhet genom deras livscykel. Förslaget syftar även till att konsumenter ska få tillräcklig information om cybersäkerheten för de produkter med digitala inslag som de köper och använder.

Ekonomiska operatörer, vilket i huvudsak är tillverkare, importörer och distributörer, ska följa de cybersäkerhetskrav förordningen anger för alla produkter med digitala inslag för att de ska kunna göras tillgängliga på den inre marknaden. Kraven innebär att tillverkare ska ta cybersäkerhet i beaktande i designen och utvecklingen av produkter med digitala inslag. Därtill ska tillverkare granska säkerhetsaspekter under utvecklingsprocessen, ha transparens gentemot konsumenter gällande cybersäkerhetsaspekter samt försäkra säkerhetssupport och uppdateringar på ett proportionerligt sätt under produktens livscykel. Regelefterlevnad uppvisas genom en konformitetsbedömning.

Förslaget kommer att medföra kostnader och nya uppgifter för myndigheter på nationell och EU-nivå som föreslås få ansvar att granska, bedriva tillsyn och upprätthålla de krav som ställs i förordningen. Det krävs ytterligare analys för att bedöma den administrativa bördan för berörda myndigheter i Sverige samt en analys gällande förslagen om nya uppgifter till myndigheter eller inrättande av nya myndigheter. Förslaget till förordning kommer sannolikt att öka den administrativa bördan för företag.

Regeringen är preliminärt positiv till förslaget och ansatsen att skapa enhetlig reglering för cybersäkerhet för produkter med digitala inslag i syfte att undvika fragmentering och stärka den inre marknadens konkurrenskraft och funktion. Regeringen ser att cybersäkerhetskrav är en nödvändig förutsättning för att digitaliseringen av samhället ska bli säker, trygg och inkluderande. Regeringen välkomnar därmed att produkter på den inre marknaden i stor utsträckning ska vara cybersäkra genom hela leveranskedjan och livscykeln.

Förordningens omfattning och administrativa bördor behöver beaktas så att de inte hämmar innovation eller blir oproportionerligt betungande för små och medelstora företag eller myndigheter. Det är viktigt för regeringen att förordningens effekter inte bidrar till flaskhalsar som försämrar konkurrenskraften för europeiska företag. Vidare anser regeringen att principer om budgetrestriktivitet, kostnadseffektivitet och samhällsekonomisk effektivitet ska beaktas.

1 Förslaget

1.1 Ärendets bakgrund

År 2020 tillkännagavs det i EU:s cybersäkerhetsstrategi för det digitala decenniet att nya regler om gemensamma europeiska cybersäkerhetsstandarder för uppkopplade produkter och tillhörande tjänster på den inre marknaden skulle införas. I sitt tal om tillståndet i unionen 2021 tillkännagav också kommissionens ordförande Ursula von der Leyen att en ny europeisk lag om cyberresiliens skulle presenteras inom ramen för kommissionens arbetsprogram 2022.

Mot bakgrund av ett växande antal uppmärksammade cyberattacker med gränsöverskridande konsekvenser uppskattades den globala årliga kostnaden för it-brottslighet uppgå till 5,5 biljoner euro för 2021. EU:s regelverk för produkter är inte utformade för att hantera de utmaningar som är specifikt kopplade med cybersäkerhet för produkter med digitala inslag. Regelverket täcker dessutom inte krav under produkternas hela livscykel. Det saknas därmed en helhetssyn som säkerställer att alla delar av en produkt med digitala inslag är cybersäkra och som även omfattar icke-inbäddade programvaruprodukter.

Kommissionen motiverar på ovanstående sätt att det finns ett behov av horisontell reglering på EU-nivå för att minimera riskerna för cyberattacker samt skapa säkrare digitala produkter för europeiska konsumenter och användare. En ny förordning skulle enligt kommissionen också gynna den inre marknaden genom att förbättra rättssäkerheten och tillhandahålla lika villkor för tillverkare och leverantörer av produkter med digitala inslag. Kommissionen anger att detta också framhålls i slutrapporten från *Konferensen om Europas framtid* där medborgarna efterlyser en starkare roll för EU i att motverka cybersäkerhetshot.

Kommissionen presenterade en förstudie den 15 december 2021 och genomförde riktade konsultationer samt offentligt samråd under första halvan av 2022. Förslaget till förordning presenterades den 15 september 2022.

1.2 Förslagets innehåll

Förslaget till förordning ämnar skapa förutsättningar för utveckling av säkra produkter med digitala inslag genom att säkerställa att hård- och mjukvara placeras på marknaden med färre sårbarheter och att tillverkare tar större ansvar för produkters säkerhet under hela deras livscykel. Förslaget ämnar även att skapa förutsättningar för konsumenter att ta cybersäkerhet i beaktande vid köp och användning av produkter med digitala inslag.

Förslaget har fyra specifika mål;

1) att säkerställa att tillverkare förbättrar säkerheten av produkter med digitala inslag från design- och utvecklingsfasen och genom livscykeln,

2) att säkerställa ett enhetligt cybersäkerhetsramverk som kan underlätta regelefterlevnad för hård- och mjukvaruproducenter,

3) att säkerställa transparens i fråga om säkerhetsegenskaper i produkter med digitala inslag, och

4) att möjliggöra för företag och konsumenter att använda produkter med digitala inslag på ett säkert sätt.

Tillverkare av produkter med digitala inslag ska rapportera kända aktivt utnyttjade sårbarheter och incidenter som påverkar produktens säkerhet till Europeiska unionens cybersäkerhetsbyrå (Enisa) inom 24 timmar från och med att sårbarheten eller incidenten kommit till kännedom.

Förordningsförslaget baseras på *New Legislative Framework* (NLF) och harmoniserade standarder som krav på tillverkare av produkter med digitala inslag att följa för att kunna sälja produkterna på inre marknaden. Självvalidering och konformitetsbedömning genom anmälda organ är den föreslagna efterlevnadsmodellen, kompletterad med marknadsövervakning.

Förslaget innehåller åtta kapitel och sex bilagor. En sammanfattning av kapitlen följer nedan.

Kapitel I anger
1) regler för att placera produkter med digitala inslag på marknaden för att försäkra dess cybersäkerhet,
2) väsentliga krav för design, utveckling och tillverkning av produkter med digitala inslag samt skyldigheter gentemot ekonomiska operatörer gällande cybersäkerhet,
3) väsentliga krav för sårbarhetshanteringsprocessen för produkter med digitala inslag genom hela livscykeln och ekonomiska operatörers skyldigheter i dessa processer, och
4) regler för marknadsövervakning och tillsyn av ovan nämnda regler.

Här fastslås även att denna förordning inte gäller produkter med digitala inslag som regleras av förordning (2017/745) om medicintekniska produkter, förordning (2017/746) om medicintekniska produkter för in vitro-diagnostik, förordning (EU) 2019/2144) om krav för typgodkännande av motorfordon, eller produkter som har varit certifierade i enlighet med förordning (2018/1139) om civila luftfartsområdet och inrättande av Europeiska unionens byrå för luftfartssäkerhet.

En kritisk produkt med digitala inslag definieras som en produkt som utgör en cybersäkerhetsrisk i enlighet med kriterierna i artikel 6.2 och vars kärnfunktioner anges i bilaga III. Kritiska produkter föreslås vara föremål för specifika konformitetsbedömningar och ska delas in i klass I och II som reflekterar deras cybersäkerhetsrisknivå. Klass II representerar en större risk och klassificeras som de mest kritiska produkterna.

Kapitel II anger de skyldigheter som ekonomiska operatörer har. Med ekonomiska operatörer avses i huvudsak tillverkare, importörer och distributörer. De väsentliga cybersäkerhetskraven och skyldigheterna innebär att alla produkter med digitala inslag ska fylla dessa krav för att göras tillgängliga på den inre marknaden. De väsentliga kraven innebär att tillverkare ska ta cybersäkerhet i beaktande i designen och utvecklingen av produkter med digitala inslag. Därtill ska tillverkare granska säkerhetsaspekter under utvecklingsprocessen, ha transparens gentemot konsumenter gällande cybersäkerhetsaspekter samt försäkra säkerhetssupport och uppdateringar på ett proportionerligt sätt.

Kapitel III anger att produkter med digitala inslag ska antas vara i överensstämmelse (presumtion om överensstämmelse) med de väsentliga kraven i detta förslag, om de är förenliga med befintliga harmoniserade standarder. I de fall harmoniserade standarder inte finns eller är otillräckliga, kan kommissionen genom genomförandeakter anta s.k. gemensamma specifikationer (som har samma status och effekt som harmoniserade standarder).

Produkter med digitala inslag som har certifierats under en europeisk cybersäkerhetscertifieringsordning ska antas vara i överensstämmelse med de väsentliga kraven i förslaget. För att underlätta eventuella administrativa bördor för tillverkare ska kommissionen, när det är applicerbart, specificera om ett cybersäkerhetscertifikat som är utfärdat under en europeisk cybersäkerhetscertifieringsordning, ger tillverkaren undantag från skyldigheterna att genomföra en konformitetsbedömning genom anmälda organ.

Tillverkare ska genomföra en konformitetsbedömning av såväl produkter med digitala inslag som sårbarhetshanteringsprocessen, för att kunna uppvisa konformitet med förslagets väsentliga krav. Tillverkare av kritiska produkter i klass II måste alltid låta genomföra en konformitetsbedömning genom anmälda organ, d.v.s. en tredjepartsgranskning.

Kapitel IV anger kraven för nationella myndigheter och ansvariga organ för konformitetsbedömning. Förslaget lämnar ansvaret för utformandet av dessa krav till medlemsstaterna. Medlemsstater ska upprätta eller utse en anmälande myndighet som ska ansvara för utförandet av de nödvändiga processerna för bedömning och notifiering av organ för konformitetsbedömning och dessa aktörers kontroll.

Kapitel V anger att nationella tillsynsmyndigheter ska utföra marknadsövervakning och tillsyn inom medlemsstatens territorium.

Kapitel VI fastslår att kommissionen har rätt att anta delegerade akter i syfte att kunna uppdatera listan av kritiska produkter med digitala inslag och att specificera definitionen av dessa produkter samt eventuella undantag.

Här fastslås också att kommissionen har mandat att anta genomförandeakter för att bland annat;
1) specificera former för rapporteringsskyldigheter,
2) specificera vilka europeiska cybersäkerhetscertifieringsordningar som kan användas för att uppvisa konformitet med de väsentliga kraven i förslaget,
3) anta gemensamma specifikationer och teknisk specificering för CE-märkning, och
4) utfärda korrigerande och begränsande åtgärder på EU-nivå i undantagsfall som rättfärdigar omedelbar intervention för att upprätthålla den interna marknadens funktion.

Kapitel VII fastslår att nationella tillsynsmyndigheter ska ha mandat att ålägga sanktioner. Förslaget anger att sanktionsavgifter till följd av bristande regelefterlevnad bör specificeras i nationell rätt.

Kapitel VIII anger tidsramen för när förordningen ska bli tillämplig, vilket är två år efter att den har trätt i kraft. Rapporteringskravet för tillverkare är dock tillämpligt redan efter ett år.

1.3 Gällande svenska regler och förslagets effekt på dessa

Den föreslagna regleringen är en förordning och blir till alla delar bindande och direkt tillämplig i varje medlemsstat. Förordningen kommer att behöva kompletteras med nationella bestämmelser, till exempel gällande nya uppgifter för vissa myndigheter. Det föreligger i nuläget inte någon närmare bedömning av i vilken omfattning sådana kompletteringar kommer att behövas.

Det finns ingen motsvarande befintlig svensk lagstiftning om cybersäkerhetskrav för samtliga produkter med digitala inslag. Vissa svenska verksamheter kommer att omfattas av krav på certifiering av produkter i enlighet med exempelvis cybersäkerhetsakten[1] (EU-förordning 2019/881). Dessa verksamheter kan eventuellt komma att också omfattas av denna förordning. I dessa fall kommer den befintliga certifieringen inom ramen för cybersäkerhetsakten förutsättas möta eventuella konformitetskrav i förordningen.

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 (marknadskontrollförordningen) fastställer ett ramverk för marknadskontroll av produkter och samarbete mellan marknadskontrollmyndigheter. Förslaget kommer att ändra marknadskontrollförordningen i vissa avseenden.

Kommissionens delegerade förordning (EU) 2022/30 av den 29 oktober 2021 om komplettering av Radioutrustningsdirektivet (2014/53/EU) anger så kallade cybersäkerhetskrav på vissa kategorier av radioutrustning. Kraven kommer att gälla från och med den 1 augusti 2024. För att undvika dubbelreglering med anledning av de nya regler som nu föreslås avser kommissionen att ändra eller upphäva nämnd förordning (jfr skäl 15 i förordningsförslaget).

1.4 Budgetära konsekvenser / Konsekvensanalys

Förslaget kommer att medföra kostnader och nya uppgifter för myndigheter på nationell och EU-nivå som föreslås få ansvar att granska, bedriva tillsyn och upprätthålla de krav som ställs i förordningen. Det krävs ytterligare

[1] Förordning om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (cybersäkerhetsakten).

analys för att bedöma den administrativa bördan för berörda myndigheter i Sverige samt en analys gällande förslagen om nya uppgifter till myndigheter eller inrättande av nya myndigheter. Eventuella kostnader som förslagen kan leda till för den nationella budgeten ska finansieras i linje med de principer om neutralitet för statens budget som riksdagen beslutat om (prop. 1994/95:40, bet. 1994/95FiU5, rskr. 1994/95:67). Utgiftsdrivande åtgärder på EU-budgeten behöver finansieras genom omprioriteringar i den fleråriga budgetramen (MFF). Förslaget förväntas inte ha budgetära konsekvenser för kommuner och regioner.

Förslaget till förordning kommer sannolikt att öka den administrativa bördan för företag. I kommissionens sammanfattning av konsekvensanalysen (SWD (2022) 283) bedömer kommissionen att förordningen kommer att medföra kostnader som är förknippade med efterlevnad av kraven, tillsyn och granskning för ekonomiska operatörer, certifieringsorgan och myndigheter. För utvecklare och tillverkare bedöms kostnaderna öka på grund av nya cybersäkerhetskrav, konformitetsbedömning, dokumentation och rapporteringsskyldigheter, vilket leder till aggregerade efterlevnadskostnader som enligt kommissionen beräknas uppgå till cirka 29 miljarder euro. På sikt beräknar kommissionen att initiativet däremot skulle kunna leda till kostnadsbesparingar på uppemot 180–290 miljarder euro årligen till följd av färre incidenter. För slutanvändare, konsumenter och medborgare kan detta innebära högre priser på produkter med digitala inslag. Dessa bör dock enligt kommissionen ses mot bakgrund av de betydande fördelarna som krav på cybersäkra produkter ger. Små och medelstora företag bedöms påverkas av de nya kraven både som tillverkare och slutanvändare. Beträffande efterlevnadskostnader skulle små och medelstora företag i princip drabbas mer än stora företag som vanligtvis har stordriftsfördelar och en större medvetenhet om cybersäkerhet. Om man emellertid ser små och medelstora företag som användare så menar kommissionen att de skulle gynnas av förordningen, eftersom cybersäkra produkter med digitala inslag skulle innebära kostnadsbesparingar. I egenskap av tillverkare skulle små och medelstora företag också gynnas av större förtroende hos slutanvändare och nya kunder. I konsekvensanalysen konstateras det även att en sömlös tillgång till den inre marknaden och en minskning av marknadsfragmenteringen kan vara ännu mer fördelaktigt för små och medelstora företag, eftersom de är sämre rustade att hantera olika regulatoriska krav.

2 Ståndpunkter

2.1 Preliminär svensk ståndpunkt

Regeringen ställer sig preliminärt positiv till förslaget i stort och till den horisontella ansats som föreslås, även om djupare analys av förslaget behövs. Regeringen är övervägande positiv till kommissionens arbete med att skapa enhetlig reglering för cybersäkerhet för produkter med digitala inslag i syfte att undvika fragmentering och stärka den inre marknadens konkurrenskraft

och funktion. Regeringen ser att cybersäkerhetskrav är en nödvändig förutsättning för att digitaliseringen av samhället ska bli säker, trygg och inkluderande. Regeringen välkomnar därmed att produkter på den inre marknaden i stor utsträckning ska vara cybersäkra genom hela leveranskedjan och hela livscykeln. Det är viktigt för ett fortsatt konkurrenskraftigt, säkert och hållbart Europa.

Enhetliga regler baserat på befintliga ramverk såsom NLF, kan skapa igenkänning, tydlighet och förutsebarhet vilket är positivt för såväl tillverkare som användare av produkter med digitala inslag. Det är emellertid viktigt att reglerna är proportionerliga i förhållande till de syften som anges, och utgår från principen om teknikneutralitet. Det är viktigt att förordningen eftersträvar en harmonisering med närliggande EU-lagstiftningsförslag som exempelvis Cybersäkerhetsakten, NIS2[2] och AI-förordningen.

Regeringen noterar att kommissionens förslag om att förordningen ska omfatta samtliga produkter med digitala inslag är mycket ambitiös och sannolikt kommer resultera i högre produktkostnader, längre ledtider och nya myndighetsuppgifter. Regeringen hoppas att förordningen samtidigt ska bidra till att kostnader förknippade med incidenter blir lägre på sikt. För att tillse att förordningen leder till önskad måluppfyllelse finns det anledning att i de fortsatta förhandlingarna verka för att kraven blir tydligt formulerade och proportionerliga samt att tillverkare av icke kritiska produkter kan uppnå regelefterlevnad utan att drabbas av betungande administrativa krav och kostnader. Regeringen noterar att förordningen ställer krav på att certifieringsorgan har tillräcklig kapacitet för att kunna hantera de nya uppgifterna. Det är viktigt för regeringen att förordningens effekter inte blir innovations- och affärsutvecklingshämmande eller bidrar till flaskhalsar som försämrar konkurrenskraften för europeiska företag. Vidare bedömer regeringen att det är viktigt att inom ramen för förhandlingarna verka för ett adekvat skydd för känslig företags- och produktinformation som kan skada företaget om den sprids.

För regeringen är det viktigt att Sverige i förhandlingarna av förslaget verkar för att förordningen inte hindrar medlemsstaterna från att vidta de åtgärder som de anser är nödvändiga för att skydda den nationella säkerheten. Vidare är det viktigt att bevaka att förordningens regler om rapportering inte strider mot medlemsstaternas säkerhetsintressen.

Regeringen anser att regleringen av harmoniserade standarder bör vara tydlig, ändamålsenlig, transparent och framtidsorienterad. Det är därför viktigt att internationella standardiseringsprinciper om öppenhet och delaktighet beaktas. Vidare anser regeringen att principer om budgetrestriktivitet, kostnadseffektivitet och samhällsekonomisk effektivitet ska beaktas. Förordningens omfattning och administrativa bördor behöver

[2] Europaparlamentets och rådets direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, och om upphävande av direktiv (EU) 2016/1148.

beaktas så att de inte hämmar innovation eller blir oproportionerligt betungande för små och medelstora företag eller myndigheter, något som i sin tur kan negativt påverka möjligheterna till ökad cybersäkerhet.

Regeringen noterar att förordningsförslaget på flera ställen ger kommissionen befogenhet att anta delegerade akter. I frågor som kan vara av betydelse för medlemsstaternas cybersäkerhetsarbete, som exempelvis kategorisering av kritiska produkter samt vilka produkter som ska omfattas av förordningen, kan det vara lämpligare att beslut tas enligt förfarandet i förordning (EU) 182/2011 (genomförandeakter).

2.2 Medlemsstaternas ståndpunkter

Flera medlemsstater har efterfrågat en horisontell reglering för att upprätta och harmonisera krav på cybersäkerhet för digitala produkter, processer och tjänster i EU. Ett antal medlemsstater har uttalat stöd för en ny europeisk cyberresiliensakt som ett användbart verktyg för att höja nivån av konsumentförtroende och informerade användare, och för att ge bättre skydd mot cyberbedrägerier, missbruk och funktionsfel.

2.3 Institutionernas ståndpunkter

Institutionernas ståndpunkter om förslaget till förordning är inte kända.

2.4 Remissinstansernas ståndpunkter

Lagförslaget har inte gått ut på remiss.

3 Förslagets förutsättningar

3.1 Rättslig grund och beslutsförfarande

Den rättsliga grunden för förslaget är artikel 114 i fördraget om Europeiska unionens funktionssätt (FEUF). Ordinarie lagstiftningsförfarande ska tillämpas, vilket innebär att rådet beslutar med kvalificerad majoritet och att Europaparlamentet är medbeslutande.

3.2 Subsidiaritets- och proportionalitetsprincipen

Cybersäkerheten för produkter med digitala inslag har en gränsöverskridande dimension, då exempelvis produkter som tillverkas i ett land ofta används på hela den inre marknaden. Den gränsöverskridande aspekten samt det ökade antalet cyberincidenter som får konsekvenser över sektors-, produkt- och nationsgränserna gör att kommissionen anser att förordningens syften inte kan uppnås på ett effektivt sätt av medlemsstaterna själva. Kommissionen anser att nationella regler potentiellt riskerar att hämma en öppen och

konkurrenskraftig inre marknad för produkter med digitala inslag. Åtgärder på EU-nivå anses därför vara nödvändiga såväl för att öka förtroendet bland användarna som attraktionskraften hos EU-produkter med digitala inslag.

Kommissionen anser mot denna bakgrund att förslagets syften bäst kan uppnås på unionsnivå genom en förordning och bedömer därför att förslaget är förenligt med subsidiaritetsprincipen. Kommissionen framför vidare att de föreslagna ändringarna inte går utöver vad som är nödvändigt för att uppnå de fastställda målen och anser därmed att förslaget är proportionerligt. Regeringen instämmer i kommissionens övergripande bedömningar rörande subsidiaritet och proportionalitet. I synnerhet förordningens proportionalitet kommer fortsatt bevakas under förhandlingens gång.

4 Övrigt

4.1 Fortsatt behandling av ärendet

Förslaget kommer att förhandlas i den horisontella rådsarbetsgruppen för cyberfrågor. Behandlingen av förslaget inleddes den 21 september 2022. Förslaget kommer troligen att förhandlas under Sveriges EU-ordförandeskap den 1 januari till och med den 30 juni 2023.

Utskottet för industrifrågor, forskning och energi (ITRE) har utsetts som ansvarigt för Europaparlamentets beredning av förslaget.

4.2 Fackuttryck/termer

Aktivt utnyttjad sårbarhet - en sårbarhet som det finns tillförlitligt bevis för att en aktör har utfört skadlig kod på ett system utan tillstånd från systemägaren.

Anmälande myndighet - den nationella myndighet som ansvarar för att inrätta och utföra de nödvändiga förfarandena för bedömning, utnämning och anmälan av organ för bedömning av överensstämmelse och för deras kontroll.

Anmält organ - ett organ för bedömning av överensstämmelse som utsetts i enlighet med artikel 33 i denna förordning och annan relevant unionslagstiftning om harmonisering.

Bedömning av överensstämmelse - processen för att kontrollera om de väsentliga kraven i bilaga I har uppfyllts.

CE-märkning - avser en märkning genom vilken en tillverkare anger att en produkt med digitala inslag och tillverkarens processer är i överensstämmelse med de väsentliga krav som anges i bilaga I och annan

tillämplig Unionslagstiftning som harmoniserar villkoren för marknadsföring av produkter.

Ekonomiska operatörer - betyder tillverkaren, den auktoriserade representanten, importören, distributören eller någon annan fysisk eller juridisk person som är föremål för skyldigheter som fastställs i denna förordning.

Kritisk produkt med digitala inslag - betyder en produkt som utgör en cybersäkerhetsrisk i enlighet med kriterierna i artikel 6.2. och vars kärnfunktioner anges i bilaga III.

Mycket kritisk produkt med digitala inslag - produkt som utgör en cybersäkerhetsrisk i enlighet med kriterierna i artikel 6(5).

Organ för bedömning av överensstämmelse - organisationer eller myndigheter som EU-länderna har utsett för att bedöma vissa produkters överensstämmelse med kraven innan de får säljas.