U 83/2022 rd

Statsrådets skrivelse till riksdagen om kommissionens förslag till Europaparlamentets och rådets förordning om horisontella krav på cybersäkerhet för produkter med digitala element (cyberresiliensakten)

I enlighet med 96 § 2 mom. i grundlagen översänds till riksdagen kommissionens förslag av den 15 september 2022 till Europaparlamentets och rådets förordning om horisontella krav på cybersäkerhet för produkter med digitala element och om ändring av förordning (EU) 2019/1020 samt en promemoria om förslaget.

Helsingfors 10.11.2022

Kommunikationsminister Timo Harakka

Specialsakkunnig Outi Slant

KOMMUNIKATIONSMINISTERIET | PROMEMORIA | EU/2022/1203

10.11.2022

KOMMISSIONENS FÖRSLAG TILL EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING OM HORISONTELLA KRAV PÅ CYBERSÄKERHET FÖR PRODUKTER MED DIGITALA ELEMENT OCH OM ÄNDRING AV FÖRORDNING (EU) 2019/1020

1 Bakgrund

Den 15 september 2022 antog kommissionen ett förslag till Europaparlamentets och rådets förordning om horisontella krav på cybersäkerhet för produkter med digitala element och om ändring av förordning (EU) 2019/1020 (KOM(2022) 454 slutlig), dvs. cyberresiliensakten.

Bakgrunden till förslaget är utvecklingen inom cybersäkerheten, som har lett till att hårdvara och mjukvara allt oftare utsätts för cyberattacker, vilket orsakar betydande kostnader för den som attackeras samt andra olägenheter som att personuppgifter äventyras. En gemensam nämnare för dessa produkter är en låg datasäkerhetsnivå i form av stora sårbarheter och bristfälliga uppdateringar samt användarnas otillräckliga insikter i produkternas säkerhetsegenskaper och begränsad tillgång till den informationen. Det här gör det svårt för konsumenterna att jämföra produkterna och deras säkerhetsegenskaper.

Utsläppandet av produkter på marknaden har en starkt gränsöverskridande dimension, samtidigt som också säkerhetsöverträdelser som rör produkterna kan ha stora gränsöverskridande konsekvenser, och därför har man ansett att det behövs bestämmelser på unionsnivå. Gemensamma åtgärder på EU-nivå har betraktats som nödvändiga för att öka förtroendet för produkterna och göra produkter som uppfyller EU-kraven attraktivare.

2 Förslagets syfte

Förslagets allmänna syfte är att skapa förutsättningar för utveckling av säkra produkter med digitala element samt säkerställa att hårdvara och mjukvara innehåller färre sårbarheter och att tillverkarna tar säkerhetsaspekterna på allvar under hela produktens livscykel. Ett ytterligare syfte är att skapa förutsättningar för konsumenterna att beakta cybersäkerhetsaspekterna när de väljer produkter med digitala element.

Förslagets specifika mål är att säkerställa produkternas säkerhet under hela deras livscykel, garantera en enhetlig ram för säkerhetskraven, främja säkerhetsegenskapernas transparens och möjliggöra säker användning av produkterna.

3 Förslagets huvudsakliga innehåll

I förslaget anges allmänna säkerhetskrav för produkter med digitala element. Förslaget innehåller skyldigheter för tillverkare, importörer och distributörer. Det innehåller också bestämmelser om bedömning av överensstämmelse, organ för bedömning av överensstämmelse, marknadskontroll och genomförande samt påföljdsavgifter.

3.1 Allmänna bestämmelser

Enligt kommissionens förslag fastställs i rättsakten cybersäkerhetsregler för produkter med digitala element som släpps ut på marknaden. Rättsakten föreslås innehålla de viktigaste kvalitetskraven på utformning, utveckling och produktion av sådana produkter och skyldigheter för kommersiella aktörer i förhållande till dessa produkter. I förslaget ingår de viktigaste processerna för hantering av sårbarheter på ett sätt som täcker hela produktens livscykel. Förslaget innehåller också regler för marknadskontrollen och för genomförandet av bestämmelserna.

Förordningen ska enligt förslaget tillämpas på produkter med ett digitalt element som kan anslutas till en annan enhet eller direkt till nätet. Anslutningen kan antingen göras direkt till exempel med fysiska kablar eller trådlöst. I princip hör alla sådana produkter till förordningens tillämpningsområde, om det inte föreskrivs särskilt om undantag. Vissa produkter med cybersäkerhetskrav som har fastställts heltäckande i EU-lagstiftning som nyligen trätt i kraft omfattas inte av förordningens tillämpningsområde. Dessa är medicintekniska produkter som omfattas av förordning (EU) 2017/745 och medicintekniska produkter för in vitro-diagnostik som omfattas av förordning (EU) 2017/746. Även motorfordon och släpvagnar som omfattas av säkerhetsförordningen för fordon (EU) 2019/2144 har lämnats utanför tillämpningsområdet. Bestämmelserna tillämpas inte heller på produkter som har ett digitalt element och omfattas av standardiseringen enligt förordningen om gemensamma bestämmelser på det civila luftfartsområdet (EASA-förordningen (EU) 2018/1139), till exempel de flesta civila luftfartyg. Förordningen tillämpas inte heller på produkter som tillverkats uteslutande för den nationella säkerhetens eller försvarets ändamål eller uttryckligen för att hantera sekretessbelagd information. Förordningen föreslås inte tillämpas på något annat än utsläppande av produkter på marknaden inom ramen för kommersiell verksamhet.

Säkerhetskraven i förslaget kan i vissa fall tillämpas begränsat eller inte alls. Det är fallet om man beaktar motsvarande krav i bestämmelser om en produkt som omfattas av unionslagstiftningen så att kraven i detta förslag helt eller delvis uppfylls. Begränsad tillämpning är möjlig om regelverket förblir enhetligt och om cybersäkerhetsnivån i de andra bestämmelserna är densamma som i förslaget. Begränsning och uteslutning görs genom kommissionens delegerade akter.

Enligt förslaget avses med produkter med digitala element vilken som helst mjukvara eller hårdvara och anknytande lösningar för fjärrbearbetning av data inklusive mjukvaru- eller hårdvarukomponenter som släpps ut på marknaden separat. Med ekonomisk aktör avses en tillverkare, en tillverkares representant, en importör, en distributör eller vilken som helst fysisk eller juridisk person som kraven i förordningen gäller. Med tillverkare avses en fysisk eller juridisk person som utvecklar eller tillverkar produkter med digitala element eller låter produkter med digitala element tillverkas under sitt namn eller varumärke antingen gratis eller mot betalning.

Medlemsstaterna får inte förhindra tillhandahållandet på marknaden om en produkt uppfyller kraven i förordningen. En i förordningen avsedd produkt får släppas ut på marknaden endast om den och processerna i anslutning till den uppfyller kraven i bilaga I till förordningen. Avvikelser från kraven kan göras bland annat i utställnings- eller demonstrationssyfte eller för begränsad testning av halvfärdig mjukvara, om det tydligt framgår att produkten inte uppfyller kraven i förordningen.

I bilaga III till förslaget till förordning definieras kritiska produkter med digitala element. Dessa produkter är indelade i två klasser enligt den risk som är förknippad med dem. Till klass I hör bland annat mjukvara och hårdvara för att hantera identitetsskydd och skydd av programvara. Dit hör också nätadministrationssystem och system för hantering av uppdateringar. Till klass I hör till exempel routrar, modem och mikroprocessorer samt system för industriell automation, om de inte av särskilda skäl hör till klass II. I klass II finns produkter med högre risk, bland

annat operativsystem för servrar och mobila enheter, olika mikroprocessorer, infrastruktur för kryptering med öppen nyckel, smartkort och system för industriell automation eller uppkopplade enheter hos aktörer som omfattas av direktivet om säkerhet i nätverk och informationssystem (NIS2-direktivet, COM (2020) 823 final). Särskilda processer för bedömning av överensstämmelse anges för båda produktkategorierna. Kommissionen ska enligt förslaget kunna anta delegerade akter om ändring av bilaga III. Om bilagan ändras ska kommissionen ta hänsyn till nivån på cybersäkerhetsrisken för produkter i den berörda kategorin. I förordningen anges kriterier för bedömningen av risknivån, bland annat att produkten kan komma att användas av i NIS2-direktivet avsedda väsentliga entiteter i deras verksamheter eller att produkten är väsentlig för leveranskedjan.

I artiklarna 7–9 i förslaget klarläggs förordningens förhållande till vissa andra rättsakter som gäller produkter, såsom den allmänna produktsäkerhetsförordningen (COM (2021) 346 final), den föreslagna AI-förordningen (COM (2021) 206 final) och den föreslagna maskinförordningen (COM (2021) 202 final). Med stöd av den föreslagna artikel 7 tillämpas huvudsakligen kraven i den allmänna produktsäkerhetsförordningen på produkter med digitala element, och dessa konsumentprodukters överensstämmelse med datasäkerhetskraven kan visas med de förfaranden som anges i cyberresiliensakten. Enligt den föreslagna artikel 8 ska vissa system för artificiell intelligens som uppfyller kraven i cyberresiliensakten anses uppfylla också de cybersäkerhetskrav som fastställs i AI-förordningen. På dessa produkter tillämpas dock bedömning av överensstämmelse enligt antingen AI-förordningen eller cyberresiliensakten, beroende på vilken typ av risk produkten är behäftad med. Med stöd av den föreslagna artikel 9 ska produkter som omfattas av tillämpningsområdet för både förslaget till maskinförordning och förslaget till cyberresiliensakt och som ska ha en EU-försäkran om överensstämmelse i enlighet med cyberresiliensakten anses uppfylla vissa datasäkerhetskrav i maskinförordningen. De ovannämnda kraven i förslaget till maskinförordning behandlar hur produkter som hör till maskinförordningens tillämpningsområde ska skyddas mot förvanskning samt tillförlitligheten i ett styrsystem för maskinernas säkerhet.

3.1 Skyldigheter för ekonomiska aktörer

Tillverkaren av en produkt som omfattas av tillämpningsområdet ska innan produkten släpps ut på marknaden försäkra sig om att produkten uppfyller kraven i bilaga 1 till förordningen. Till dessa krav hör att produkterna ska utformas, utvecklas och produceras så att deras säkerhetsnivå står i rätt proportion till riskerna. Produkterna får inte innehålla några kända sårbarheter. Bilagan innehåller också mer detaljerade krav som gäller till exempel databehandling och avvärjande av risker. Tillverkarna ska bedöma produkternas cybersäkerhetsrisker och beakta bedömningen under produktens hela livscykel, från utformning till användning och underhåll, samt minimera alla cybersäkerhetsrisker och riskernas eventuella konsekvenser. När produkter släpps ut på marknaden ska tillverkaren inkludera en bedömning av cybersäkerhetsriskerna i den tekniska dokumentationen. Tillverkaren ska försäkra sig om att komponenter som levererats av tredje parter inte äventyrar produktens säkerhet. Faktorer som påverkar cybersäkerheten och blir kända, till exempel sårbarheter, ska dokumenteras. Produkternas sårbarheter ska hanteras under hela produktens livscykel eller fem år efter utsläppandet på marknaden, beroende på vilken period som är kortare. Säkerhetsaspekterna ska dokumenteras och produktens överensstämmelse med kraven ska bedömas. En EU-försäkran om överensstämmelse ska lämnas om att kraven uppfylls, och produkten ska CE-märkas.

Enligt förslaget ska användaren få information och anvisningar enligt bilaga II, inklusive produktens och tillverkarens kontaktuppgifter samt bland annat uppgifter om hur man får information om produktens eventuella sårbarheter. Om det under produktens livscykel framkommer att den inte uppfyller säkerhetskraven i förordningen ska produkten justeras så att den motsvarar

kraven, eller dras tillbaka från marknaden. Tillverkaren ska samarbeta med marknadskontrollmyndigheterna. Om tillverkaren lägger ner sin verksamhet under produktens livscykel ska detta rapporteras till marknadskontrollmyndigheten och så vitt det är möjligt ska också användarna informeras.

Om en sårbarhet aktivt exploateras eller en säkerhetsöverträdelse inträffar i samband med produkten ska tillverkaren underrätta EU:s cybersäkerhetsbyrå ENISA inom loppet av 24 timmar efter ha fått kännedom om den. ENISA skickar informationen till de nationella medlemmarna i CSIRT-nätverket (Computer Security Incident Response Team) och till marknadskontrollmyndigheten. Tillverkaren ska utan ogrundat dröjsmål underrätta produktens användare om upptäckta incidenter och vid behov förklara hur användaren kan minimera skadliga konsekvenser. Tillverkaren ska underrätta komponenttillverkarna om sårbarheter som upptäckts i komponenterna.

Det viktigaste kravet på importörerna är att de i fortsättningen endast får släppa ut produkter på marknaden om produkterna uppfyller säkerhetskraven i förordningen. Importörerna ska försäkra sig om att överensstämmelsen har bedömts, den tekniska dokumentationen har gjorts och produkten har CE-märkts och innehåller de bruksanvisningar som krävs. Importörer som upptäcker säkerhetsbrister i produkter de importerar ska omedelbart vidta korrigerande åtgärder och vid behov dra tillbaka produkten från marknaden. Tillverkaren ansvarar för korrigerande åtgärder. Importören ska vid behov skicka den dokumentation som krävs till marknadskontrollmyndigheterna samt informera myndigheterna och om möjligt användarna om tillverkaren avslutar sin verksamhet och inte kan fullgöra sina skyldigheter. Liksom för importörer föreslås en skyldighet för distributörer att samarbeta med marknadskontrollmyndigheterna och informera om att tillverkaren avslutat sin verksamhet.

Distributörerna har ålagts skyldigheten att kontrollera att produkten är CE-märkt och att tillverkaren och importören iakttar de krav som ställs på dem när det gäller dokumentation och anvisningar. Produkter som inte överensstämmer med kraven får inte tillhandahållas på marknaden. Om det finns skäl att misstänka bristande överensstämmelse ska distributören vidta åtgärder på samma sätt som föreslås i fråga om importörer. Kraven på tillverkare tillämpas på importörer och distributörer till exempel om de ändrar produkten på ett betydande sätt.

Ekonomiska aktörer, till exempel distributörer, ska på begäran till marknadskontrollmyndigheten lämna uppgifter om ekonomiska aktörer som har levererat produkter med ett digitalt element till dem samt till vem de själva har levererat sådana produkter.

3.2 Produkternas överensstämmelse

Enligt förslaget ska produkter anses uppfylla kraven om tillverkaren har uppfyllt de harmoniserade standarder för produkten som publicerats i EU:s officiella tidning. Produkter som uppfyller de tekniska specifikationer som anges i förordningen anses överensstämma med de krav i förordningen som gäller säkerhet. Produkter med en EU-försäkran om överensstämmelse eller ett certifikat enligt cybersäkerhetsförordningen (EU) 2019/881 som motsvarar kraven i den föreslagna förordningen anses uppfylla förordningens säkerhetskrav. Kommissionen kan med genomförandeakter precisera cybersäkerhetsförordningens certifieringsordningar så att de motsvarar kraven i förordningen.

Om harmoniserade standarder saknas eller kommissionen betraktar dem som otillräckliga eller annars bristfälliga ska kommissionen enligt förslaget kunna anta genomförandeakter om tekniska specifikationer för de säkerhetskrav som anges i bilagan till förordningen. I fråga om CE-märkning iakttas de allmänna principerna i Europaparlamentets och rådets förordning om krav

för ackreditering och marknadskontroll i samband med saluföring av produkter (EG) nr 765/2008. Förslaget innehåller regler och villkor för anbringande av CE-märkning.

I förslaget finns närmare bestämmelser om bedömning av överensstämmelse. Förslaget utgår från att bedömningen av överensstämmelse utförs av tillverkaren som intern kontroll. Tillverkaren genomför bedömningen av överensstämmelse för att fastställa om produkten uppfyller de viktigaste kraven i bilaga I. Överensstämmelsen kan bedömas genom intern kontroll eller EU-typkontroll som genomförs av ett visst anmält organ. Om produkten är behäftad med större cybersäkerhetsrisker än normalt ska ett externt bedömningsorgan visa överensstämmelsen. Överensstämmelsen kan också visas genom fullständig kvalitetssäkring där bedömningen genomförs av ett anmält organ. I bilaga IV till förslaget till förordning finns bestämmelser om hur överensstämmelsen visas.

För produkter med hög risk, alltså kritiska produkter med digitala element, visas överensstämmelsen genom EU-typkontroll följt av bedömning av överensstämmelse som grundar sig på intern kontroll, om harmoniserade cybersäkerhetscertifikat för produkten saknas helt eller bara delvis har tillämpats. Överensstämmelsen kan också visas genom fullständig kvalitetssäkring. För synnerligen kritiska produkter med digitala element genomförs bedömningen av överensstämmelse också alltid utifrån en bedömning av ett externt anmält organ. Anmälda organ ska ta hänsyn till små och medelstora företags behov genom att för dessa fastställa rimliga avgifter för bedömning av överensstämmelse.

3.3 Anmälan av organ för bedömning av överensstämmelse

Enligt förslaget ska medlemsstaterna till kommissionen och de övriga medlemsstaterna anmäla de bedömningsorgan som får genomföra bedömning av överensstämmelse enligt förordningen. Medlemsstaterna ska tillsätta en anmälande myndighet som ansvarar för att bedöma och anmäla organ för bedömning av överensstämmelse och anmälda organ. För att undvika intressekonflikter och säkerställa opartiskheten ställs vissa krav på den anmälande myndigheten. Medlemsstaterna ska informera kommissionen om myndighetens bedömnings- och anmälningsprocess och tillsyn.

I förordningen ställs vissa krav på organ som bedömer överensstämmelse. Sådana organ ska vara juridiska personer, och både organet och dess personal ska vara oberoende av de organisationer vars produkter de bedömer. Organen ska ha tillräckligt kompetent personal, den utrustning som behövs och en beskrivning av bedömningsprocessen för att garantera processens transparens. Bedömningsverksamheten ska skiljas åt från organets eventuella andra verksamheter och den ska vara konfidentiell förutom i förhållande till marknadskontrollmyndigheten. Ett organ för bedömning av överensstämmelse anses uppfylla kraven om det uppfyller de relevanta standarder som publicerats i EU:s officiella tidning. Även underleverantörer till anmälda organ ska uppfylla de ovannämnda kraven, och de anmälda organen ansvarar för sina underleverantörers verksamhet.

Ansökan om status som organ för bedömning av överensstämmelse görs till den anmälande myndigheten. I ansökan ska organet beskriva verksamheten och de produkter som den vill bedöma. Den anmälande myndigheten anmäler de organ som uppfyller kraven till kommissionen. Kommissionen för en förteckning över bedömningsorganen. Kommissionen ska underrättas om det sker förändringar i organens kravuppfyllelse. Kommissionen kan också bedöma om ett anmält organ fortfarande är kompetent eller uppfyller kraven, om det förekommer tvivel.

Bedömningarna av överensstämmelse ska vara proportionella så att de ekonomiska aktörerna inte belastas i onödan. Vid bedömningen ska hänsyn tas till företagets storlek, bransch och

struktur, till produktens tekniska komplexitet samt till om den är avsedd för serietillverkning. Utgående från bedömningen kan organet föreslå korrigerande åtgärder så att produkten uppfyller kraven i förordningen. Kommissionen säkerställer samordningen och samarbetet mellan de bedömande organen och medlemsstaterna ser till att organen deltar i samarbetet.

3.4 Marknadskontroll och genomförande

På marknadskontrollen av produkter med digitala element tillämpas Europaparlamentets och rådets förordning (EU) 2019/1020 om marknadskontroll och överensstämmelse för produkter (marknadskontrollförordningen). Medlemsstaterna ska utse en eller flera myndigheter till marknadskontrollmyndigheter för att säkerställa ett effektivt genomförande av den föreslagna förordningen. Myndigheten får vara befintlig eller ny. Marknadskontrollmyndigheterna ska samarbeta med myndigheterna för cybersäkerhetscertifiering och regelbundet utbyta information med dem. Marknadskontrollmyndigheterna ska också samarbeta med andra relevanta myndigheter, såsom dataskyddsmyndigheter. Dataskyddsmyndigheterna har rätt att få dokumentation som upprättats med stöd av den föreslagna förordningen om dokumentationen behövs för skötseln av deras uppgifter.

Marknadskontrollmyndigheterna ska garanteras tillräckliga ekonomiska resurser och personalresurser. Myndigheterna ska årligen rapportera till kommissionen om resultaten av marknadskontrollen. Marknadskontrollen av AI-system med hög risk genomförs i enlighet med AI-förordningen, men i samarbete med de marknadskontrollmyndigheter som avses i den föreslagna förordningen. Marknadskontrollmyndigheterna ska ges tillgång till behövliga data, inbegripet intern dokumentation, för att de ska kunna bedöma överensstämmelsen. En administrativ samarbetsgrupp med representanter för marknadskontrollmyndigheterna inrättas för att säkerställa en enhetlig tillämpning av rättsakten.

En nationell marknadskontrollmyndighet som har skäl att bedöma att en produkt på marknaden utgör en betydande cybersäkerhetsrisk ska genomföra en utvärdering. Om produkten inte anses uppfylla kraven ska myndigheten underrätta den relevanta aktören så att bristerna korrigeras eller produkten vid behov dras tillbaka från marknaden. Om bristerna bedöms vara gränsöverskridande ska kommissionen och de övriga medlemsstaterna informeras. Tillverkaren ska vidta alla korrigerande åtgärder som är möjliga för att åtgärda situationen. Om nödvändiga åtgärder inte vidtas kan marknadskontrollmyndigheten förbjuda eller begränsa tillhandahållandet av produkten på marknaden. Kommissionen och de övriga medlemsstaterna ska informeras om att processen inletts och om de nationella åtgärderna. De andra medlemsstaternas marknadskontrollmyndigheter ska skicka den information som de eventuellt har om den aktuella produkten. Även oenigheter ska rapporteras. Om ingen motsätter sig inom loppet av tre månader träder de nationella åtgärderna i kraft.

Om en medlemsstat motsätter sig kontrollåtgärder som inletts av en annan medlemsstat eller om kommissionen anser att följderna strider mot unionslagstiftningen inleder kommissionen samråd mellan medlemsstaterna och med den ekonomiska aktören för att utvärdera de nationella åtgärderna. Utgående från denna utvärdering fastställer kommissionen inom loppet av nio månader om påföljden har varit befogad.

Om kommissionen har grundad anledning att misstänka att en produkt med ett digitalt element utgör en betydande cybersäkerhetsrisk kan den be den relevanta marknadskontrollmyndigheten att genomföra en utvärdering. I exceptionella situationer kan kommissionen också be ENISA att genomföra utvärderingen. Utgående från utvärderingen beslutar kommissionen om korrigerande åtgärder. Därefter samråder kommissionen med medlemsstaterna och de relevanta ekonomiska aktörerna och kan utgående från det anta genomförandeakter.

I situationer då en produkt uppfyller kraven i förordningen men ändå utgör en betydande cybersäkerhetsrisk och dessutom ett hot för människors hälsa och säkerhet, grundläggande fri- och rättigheter som tryggas i unionslagstiftningen eller nationell lagstiftning, integriteten eller konfidentialiteten för tjänster som tillhandahålls av väsentliga entiteter som avses i NIS2–direktivet eller andra aspekter av skydd i allmänhetens intresse ska medlemsstaten kräva att aktören vidtar de åtgärder som behövs för att produkten inte längre ska utgöra en sådan risk. Produkten kan också dras tillbaka från marknaden inom en rimlig tid i förhållande till typen av risk. Kommissionen och medlemsstaterna ska genast informeras om beslutet, varefter kommissionen omedelbart inleder samråd med medlemsstaterna och de relevanta ekonomiska aktörerna. Utifrån samrådet avgörs om åtgärden är proportionerlig. Kommissionen är behörig i dessa situationer och förfarandet är detsamma som i fråga om åtgärder beskrivs i föregående stycke.

Enligt förslaget till förordning förekommer följande situationer som strider mot förordningen: CE-märkningen har fästs i strid med kraven i förordningen eller inte alls, EU-försäkran om överensstämmelse har inte lämnats eller har lämnats felaktigt, bedömningsorganets uppgifter har inte bifogats eller den tekniska dokumentationen är inte tillgänglig eller färdig. I sådana situationer kan medlemsstaterna vidta behövliga åtgärder för att begränsa eller förbjuda tillverkningen av produkten eller dra tillbaka den från marknaden.

Marknadskontrollmyndigheterna kan inleda samarbete för att säkerställa cybersäkerheten och skydda konsumenterna. Ett sådant samarbete kan gälla produkter som ofta visar sig medföra cybersäkerhetsrisker. Även kommissionen och ENISA kan föreslå gemensamma åtgärder för bedömning av överensstämmelse på basis av uppgifter om eventuell bristande efterlevnad. Detta får dock inte leda till snedvridning av marknaden. Marknadskontrollmyndigheterna kan också vidta samordnade och samtidiga kontroller (sweeps) av vissa produkter eller kategorier av produkter.

3.5 Delegerade befogenheter och kommittéförfarande

I kapitlet anges kommissionens befogenheter att anta delegerade akter. Kommissionen får enligt förslaget anta delegerade akter om att inte tillämpa eller endast delvis tillämpa bilaga I på vissa produkter, om att ändra listan över kritiska produkter i bilaga III, om innehållet i EU:s försäkran om överensstämmelse enligt bilaga IV samt om innehållet i den tekniska dokumentationen enligt bilaga V. En delegering av befogenheter får när som helst återkallas av Europaparlamentet eller rådet. Kommissionen ska samråda med nationella sakkunniga i det aktuella ärendet innan en delegerad akt antas. Kommissionen biträds av en kommitté vid behandlingen av genomförandeakter i enlighet med förslaget.

3.6 Konfidentialitet och påföljder

Alla parter som deltar i tillämpningen av förordningen ska iaktta konfidentialitet i synnerhet för att skydda immateriella rättigheter och företagshemligheter, säkerställa ett effektivt genomförande, trygga den nationella och allmänna säkerheten och garantera de administrativa förfarandenas integritet. Marknadskontrollmyndigheterna får utbyta information med varandra och kommissionen. Kraven påverkar dock inte parternas skyldigheter i straffrättsliga processer. Information kan också utbytas med tredjeländer om dessa länder har ingått ett avtal om konfidentiellt informationsutbyte med EU eller en medlemsstat.

Medlemsstaterna ska fastställa påföljder för överträdelser av bestämmelserna. Enligt EU:s allmänna principer ska påföljderna vara effektiva, proportionella och avskräckande. Påföljderna är administrativa. Medlemsstaterna har handlingsutrymme när de påför administrativa påföljder, men i förslaget föreskrivs det om en skyldighet för medlemsstaterna att påföra påföljder

och om det maximala belopp som kan påföras som påföljd för verksamhet som strider mot bestämmelserna. För bristande efterlevnad av de väsentliga cybersäkerhetskraven enligt bilaga I och tillverkarnas skyldigheter enligt förordningen ska man kunna påföra en administrativ straffavgift på högst 15 miljoner euro eller 2,5 procent av årsomsättningen, enligt vilket belopp som är högst. För brott mot övriga skyldigheter är påföljden högst 10 miljoner euro eller 2 procent av årsomsättningen, enligt vilket belopp som är högst. En aktör som lämnar felaktig, vilseledande eller ofullständig information till ett bedömningsorgan ska kunna påföras en administrativ straffavgift på högst 5 miljoner euro eller 1 procent av årsomsättningen, enligt vilket belopp som är högst. När beloppet av den administrativa straffavgiften fastställs beaktas omständigheterna i det enskilda fallet, det vill säga överträdelsens art, omfattning, varaktighet och konsekvenser, den skyldiga aktörens storlek och marknadsandel samt om andra myndigheter redan har påfört motsvarande avgifter. De övriga marknadskontrollmyndigheterna ska underrättas om påföljden. Varje medlemsstat bestämmer i vilken utsträckning administrativa straffavgifter kan påföras myndigheter. Administrativa straffavgifter påförs av den myndighet som är behörig enligt det nationella systemet. Avgifterna kan påföras i samband med att andra korrigerande eller begränsande åtgärder fastställs.

3.7 Slutbestämmelser

EU-typintyg och beslut om godkännande som gäller cybersäkerhetskrav för produkter ska enligt förslaget förbli kraft i 48 månader såvida de inte löper ut tidigare eller något annat specificeras i unionslagstiftningen. Förordningen tillämpas på produkter som släppts ut på marknaden före ikraftträdandet endast om produkterna modifieras väsentligt. Skyldigheterna att rapportera sårbarheter i produkter gäller dock också produkter som släppts ut på marknaden innan förordningen träder i kraft.

Förordningen utvärderas med fyra års mellanrum och för första gången tre år efter att den börjat tillämpas. Förordningen börjar tillämpas två år efter att den trätt i kraft. Skyldigheterna att rapportera sårbarheter tillämpas dock redan från och med ett år efter ikraftträdandet.

4 Förslagets rättsliga grund och förhållande till proportionalitetsprincipen och subsidiaritetsprincipen

Förslagets rättsliga grund är artikel 114 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget), enligt vilken det får antas bestämmelser om åtgärder för tillnärmning av sådana lagar och andra författningar i medlemsstaterna som syftar till att upprätta den inre marknaden och få den att fungera. Förslaget behandlas i enlighet med det ordinarie lagstiftningsförfarandet, där Europaparlamentet och rådet tillsammans antar förordningen. I rådet förutsätts beslut med kvalificerad majoritet.

Förslagets syfte är att harmonisera medlemsstaternas cybersäkerhetskrav för produkter som omfattas av tillämpningsområdet för att eliminera hinder för varors fria rörlighet. Kommissionen har motiverat valet av rättslig grund bland annat med att den gällande EU-lagstiftning som tillämpas på vissa säkerhetsaspekter och ansvarsfrågor för produkter med digitala element baseras på artikel 114 i EUF-fördraget. Kommissionen motiverar harmoniseringsbehovet med att medlemsstaterna på nationell nivå redan har börjat kräva att försäljare av digitala produkter utvecklar cybersäkerhetsaspekterna. Samtidigt har digitala produkters cybersäkerhet en stark gränsöverskridande dimension eftersom produkterna säljs och används på hela den inre marknaden, och eventuella cyberstörningar i produkterna följaktligen också avspeglas på hela den inre marknaden. Genom förslaget harmoniseras och förenhetligas cybersäkerhetskraven för produkter med digitala element på EU:s inre marknad.

Kommissionen anser att förslaget är förenligt med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen (FEU) Enligt kommissionen kan förslagets målsättningar inte effektivt uppnås genom medlemsstaternas nationella lagstiftning eftersom cybersäkerhetshoten är internationella. Medlemsstaternas olika nationella strategier kan leda till rättslig osäkerhet och hinder för produkternas rörlighet. Ett gemensamt tillvägagångssätt inom EU stärker användarnas förtroende för produkter med digitala element och tryggar rättssäkerheten och aktörernas jämlika verksamhetsförutsättningar på den inre marknaden.

Kommissionen anser att förslaget är förenligt med proportionalitetsprincipen enligt artikel 5 i FEU och varken går utöver vad som är nödvändigt för att uppnå målen eller orsakar oproportionerliga kostnader. De krav som ställs på produkterna är rimliga, teknikneutrala och anpassade till risken, och de täcker produkternas hela livscykel. Cybersäkerhetskraven skulle via standardisering vara riskbaserade. Kommissionen bedömer att nyttan av den höjda cybersäkerhetsnivå som följer av de föreslagna bestämmelserna överväger företagens kostnader för efterlevnaden av bestämmelserna.

Statsrådets preliminära ståndpunkt är att kommissionens syn på förordningens rättsliga grund samt subsidiaritetsprincipen och proportionalitetsprincipen är korrekt. Förordningens tillämpningsområde är dock omfattande, vilket förutsätter att frågan om den rättsliga grunden behandlas under den fortsatta beredningen. Området för den regleringsmakt som delegeras till kommissionen påverkar också bedömningen.

5 Förslagets konsekvenser

5.1 Kommissionens konsekvensbedömning

Kommissionen har gjort en omfattande bedömning av alternativa handlingsvägar och deras konsekvenser för att uppnå målen med förslaget och ingripa i det bakomliggande problemet.

Enligt kommissionens konsekvensbedömning har förslaget betydande fördelar. Företagen gynnas av att förslaget förhindrar uppkomsten av varierande cybersäkerhetskrav på EU:s inre marknad, vilket minskar kostnaderna för överensstämmelsen med kraven. Förslaget minskar antalet säkerhetsöverträdelser eftersom säkerhetsnivån för produkterna på marknaden förbättras, vilket minskar kostnaderna för säkerhetsöverträdelser och utredningen av dem. Kommissionen bedömer att förslaget på EU-nivå kan sänka företagens kostnader för säkerhetsöverträdelser med upp till 180–290 miljarder euro. Förslaget ökar företagens omsättning genom att det ökar efterfrågan på produkter som hör till tillämpningsområdet och även utanför EU förbättrar anseendet för företagen och deras produkter som omfattas av tillämpningsområdet. För användarna ökar förslaget datasäkerhetsegenskapernas transparens och hjälper dem använda produkterna på ett datasäkert sätt. Konsumenterna och allmänheten gynnas också av förslagets effekter på produkterna, som förbättrar integritetsskyddet, skyddet för konfidentiell information och dataskyddet.

Kommissionen bedömer att de största nackdelarna med förslaget är kostnaderna för efterlevnaden av de nya kraven. Förslaget ökar företagens, de anmälda organens och myndigheternas kostnader för överensstämmelsen och övervakningen av överensstämmelsen. Förslaget ökar direkt behovet av ackrediteringar och arbetsmängden för den myndighet som utses till marknadskontrollmyndighet. För mjukvaruutvecklare och produkttillverkare som omfattas av tillämpningsområdet ökar förslaget direkt kostnaderna för efterlevnaden av de nya säkerhetskraven, bedömningen av överensstämmelse, dokumentationen och rapporteringen. Kommissionen uppskattar att dessa kostnader är cirka 29 miljarder euro i hela EU, då storleken på den marknad som omfattas av tillämpningsområdet är cirka 1 485 miljarder euro. Förslaget kan höja priserna

på produkter som hör till tillämpningsområdet, vilket är negativt för användarna, konsumenterna och andra köpare av program och produkter.

5.2 Nationella konsekvenser

Förslagets nationella konsekvenser för Finland och finländska aktörer bedöms noggrannare när behandlingen framskrider.

5.2.1 Konsekvenser för produkternas användare

Förslaget kommer att ha konsekvenser för konsumenterna och andra beställare och användare av produkter som omfattas av tillämpningsområdet, till exempel företag. De produkter som släpps ut på marknaden får bättre cybersäkerhetsegenskaper än i dag, och konsumenterna får bättre tillgång till information om produkternas cybersäkerhetsegenskaper, vilket medför en betydande nytta för användarna. När cybersäkerhetskraven skärps kan beställarna och användarna lita på att alla produkter har en basnivå av cybersäkerhet. Förslaget förbättrar skyddet för integriteten och förtroliga meddelanden samt dataskyddet vid elektronisk kommunikation. Man kan dock bedöma att efterlevnaden av cybersäkerhetskraven kommer att medföra nya kostnader, och därför kan produkternas pris stiga eller produktegenskaper avlägsnas om de äventyrar cybersäkerhetsnivån eller påverkar tillämpningen av kraven när produkten släpps ut på marknaden.

5.2.2 Konsekvenser för tillverkare, importörer och distributörer

Förslaget har konsekvenser för tillverkare, distributörer och importörer i Finland av produkter som omfattas av dess tillämpningsområde. I synnerhet för tillverkarna uppstår nya kostnader för överensstämmelsen med kraven. De föreslagna striktare cybersäkerhetskraven ökar kostnaderna för tillverkning, distribution och import av produkter med digitala element. Samtidigt bör det noteras att en del företag redan för närvarande iakttar liknande säkerhetsåtgärder som de föreslagna, och konsekvenserna fördelar sig därför inte jämnt på alla tillverkare. Förslaget förbättrar generellt säkerhetsnivån i en cybermiljö för produkterna på marknaden, vilket indirekt ger betydande fördelar. Dessutom uppfyller en produkt med digitala element med en gång i hela EU de gemensamma harmoniserade cybersäkerhetskraven, vilket underlättar finländska tillverkares och distributörers export till den inre marknaden och stärker deras ställning och möjligheter också på den globala marknaden. Det bör noteras att bedömningen av produktens kritiska karaktär och därigenom bedömningskraven i förslaget till förordning delvis baseras på slutanvändningen, men att tillverkaren inte alltid vet var produkten i slutändan kommer att användas. Alla ekonomiska aktörer har inte nödvändigtvis heller de resurser som behövs för att uppfylla kraven, vilket kan ha konsekvenser för affärsverksamheten.

5.2.3 Konsekvenser för de bedömande organens verksamhet

När bedömningarna av produkters överensstämmelse ökar behövs också fler bedömande organ och följaktligen också fler experter som gör bedömningarna. På nationell nivå kan det bli svårt att genomföra externa bedömningar av överensstämmelse för produkterna under övergångstiden eftersom Finland har ett begränsat antal anmälda organ som gör bedömningar av överensstämmelse. Redan nu har man insett problemet att tillgången på datasäkerhetsproffs är begränsad och konkurrensen om arbetskraft hård. Det finns också ett uppenbart utbildningsbehov bland användare, tillverkare, importörer, bedömande organ och myndigheter. I preliminära samtal med de berörda har det visat sig att bedömningen av vissa produktkategorier också förutsätter kunskaper om den aktuella branschens särdrag, vilket ytterligare minskar antalet sakkunniga personer som kan utföra datasäkerhetsbedömningar. Det finns ett uppenbart behov av sådana

personer för att nyttan med bedömningsverksamheten ska kunna uppnås. Samtidigt tillför utvidgningen av bedömningsverksamheten nya affärsmöjligheter både nationellt och på EU-nivå.

5.2.4 Konsekvenser för myndigheterna

Om förslaget genomförs har det väsentliga konsekvenser för myndigheterna. Myndighetsuppgifterna i samband med marknadskontrollen av produkter med digitala element är nya, och de förutsätter nya nationella resurser. Förslaget till förordning innehåller en uttrycklig skyldighet för medlemsstaterna att se till att marknadskontrollmyndigheterna har tillräckliga resurser. Därmed har genomförandet av förslaget budgetkonsekvenser som bedöms när förhandlingarna framskrider. Budgetkonsekvenserna kan antas vara större än ringa med beaktande av det stora antalet produkter som omfattas av förordningens tillämpningsområde och följaktligen de resurser som marknadskontrollen kräver. En annan omständighet som påverkar myndigheterna är uppgiften som ansvarig myndighet för behandlingen av ansökningar om att godkännas som anmält organ samt tillsynen över de anmälda organen. Det är sannolikt att förslaget medför ett allt större behov av bedömande organ, och då förutsätter det också i motsvarande mån en ökning av myndighetsresurserna såväl kvantitativt som kompetensmässigt.

Dataombudsmannen får merarbete till följd av den uttryckliga bestämmelsen om samarbete mellan marknadskontrollmyndigheterna och dataskyddsmyndigheterna i artikel 41 i förslaget till förordning. De exakta konsekvenserna för resursbehovet beror på i vilken mån den slutliga artikeln ålägger myndigheterna att samarbeta, och på om den föreslagna bestämmelsen innebär en ny uppgift.

Förslaget kommer sannolikt också att förutsätta kompletterande nationella bestämmelser om till exempel skyldigheter att utbyta information mellan marknadskontrollmyndigheterna, dataombudsmannen och tillsynsmyndigheterna enligt cybersäkerhetsförordningen för att myndigheterna ska kunna utföra sina uppgifter.

6 Förslagets förhållande till grundlagen samt till de grundläggande och mänskliga rättigheterna

De föreslagna bestämmelserna är relevanta med tanke på skyddet för privatlivet och skydd av personuppgifter enligt 10 § 1 mom. i grundlagen, skyddet för förtroliga meddelanden enligt 10 § 2 mom. i grundlagen som tryggas i artiklarna 7 och 8 i EU:s stadga om de grundläggande rättigheterna. Förslaget är också betydelse av näringsfriheten enligt 18 § 1 mom. i grundlagen som stiftas också i artikel 15 i stadga av grundläggande rättigheterna. Förslaget är också relevant för rättsskyddet, som tryggas i 21 § i grundlagens om säkras i artikel 47 i stadga av grundläggande rättigheterna. Det är nödvändigt att göra en bedömning också av den straffrättsliga legalitetsprincipen och föreslaget innehåller förslag till bestämmelser där en offentlig förvaltningsuppgift överförs på någon annan än en myndighet. Detta är relevant i förhållande till 124 § i grundlagen.

6.1 Skyddet för privatlivet

De cybersäkerhetskrav som föreslås för produkter med digitala element främjar skyddet för privatlivet och förtroliga meddelanden vid användningen av dessa produkter. Frågan är därför relevant för skyddet för privatlivet och förtroliga meddelanden enligt 10 § i grundlagen. Förslaget kan bedömas främja tillgodoseendet av dessa grundläggande fri- och rättigheter i synnerhet eftersom produkternas förbättrade datasäkerhetsegenskaper direkt bidrar till att bevara kommunikationens konfidentialitet och därigenom till skyddet av privatlivet. Därför är förslaget också

relevant för skyddet av personuppgifter. Enligt kommissionen bidrar de horisontella cybersäkerhetskraven i synnerhet till säkerheten för personliga data, såsom personuppgifter, genom att skydda konfidentialiteten, integriteten och tillgängligheten. Enligt skäl 17 i ingressen till förslaget till förordning bör förordningen inte påverka tillämpningen av den allmänna dataskyddsförordningen (EU) 2016/679.

6.2 Näringsfrihet och rätt till arbete

De föreslagna kraven har en dimension som inskränker näringsfriheten, eftersom produkter som inte uppfyller kraven inte tillåts på den inre marknaden. Förslaget är därför relevant för näringsfriheten, som tryggas i 18 § i grundlagen, där det föreskrivs att var och en i enlighet med lag har rätt att skaffa sig sin försörjning genom arbete, yrke eller näring som han eller hon valt fritt. Avsikten med inskränkningen av näringsfriheten är dock att förbättra datasäkerhetsegenskaperna hos produkter som släpps ut på marknaden och på det sättet främja andra skyddsintressen, och därför kan inskränkningarna betraktas som motiverade.

En annan aspekt som är relevant för näringsfriheten är att de bedömande organens verksamhet föreslås vara tillståndspliktig. Kravet på myndighetstillstånd för att utöva ett arbete, ett yrke eller en näring innebär en inskränkning av näringsfriheten, som tryggas i 18 § 1 mom. i grundlagen. Bestämmelserna om inskränkning av näringsfriheten ska vara exakta och noga avgränsade och dessutom ska inskränkningens omfattning och villkor framgå av lagen. Grundlagsutskottet har ansett det viktigt att bestämmelserna om villkoren för tillstånd och tillståndets giltighet garanterar en tillräcklig förutsägbarhet i myndigheternas verksamhet.

6.3 Rättsskydd

Enligt 21 § 1 mom. i grundlagen har var och en rätt att på behörigt sätt och utan ogrundat dröjsmål få sin sak behandlad av en domstol eller någon annan myndighet som är behörig enligt lag samt att få ett beslut som gäller hans eller hennes rättigheter och skyldigheter behandlat vid domstol eller något annat oavhängigt rättskipningsorgan. I förslaget ingår bestämmelser om marknadskontroll och genomförande som gäller vilka åtgärder som kan vidtas inom ramen för marknadskontrollen och under vilka förutsättningar. Med stöd av 2 § 3 mom. i grundlagen ska bestämmelser om myndigheternas behörighet och befogenheter utfärdas genom lag. Trots att förordningen är direkt tillämplig kan det behövas bestämmelser i nationell lag om vissa frågor som gäller till exempel myndigheternas befogenheter.

På förslaget tillämpas den allmänna marknadskontrollförordningen (EU) 2019/1020, där det i artikel 18 föreskrivs om processuella rättigheter för ekonomiska aktörer, vilket i synnerhet innebär rätten att bli hörd. På nationell nivå kompletteras marknadskontrollförordningen av den horisontella lagen om marknadskontrollen av vissa produkter (1137/2016), där det föreskrivs närmare om myndigheternas tillsynsåtgärder och bland annat förfarandet vid sökande av ändring. Sannolikt tillämpas den lagen också i fortsättningen på marknadskontrollen enligt den föreslagna förordningen.

Enligt förslaget säkerställs enhetliga åtgärder för marknadskontroll inom EU i synnerhet genom de förfaranden som ingår i artikel 44, det vill säga att kommissionen kan inleda samråd mellan medlemsstater och ekonomiska aktörer om en medlemsstat motsätter sig en marknadskontrollåtgärd. Utifrån samrådet avgör kommissionen om åtgärden är proportionerlig.

6.4 Den straffrättsliga legalitetsprincipen

I den föreslagna artikel 53 finns bestämmelser om administrativa straffavgifter för brott mot säkerhetskraven och kraven i andra förordningar och för lämnande av vilseledande eller felaktig information till en tillsynsmyndighet. Enligt grundlagsutskottets etablerade tolkning är sådana avgifter varken skatter eller avgifter med avseende på 81 § i grundlagen, utan administrativa påföljder av sanktionskaraktär för lagstridiga gärningar, och utskottet har jämställt dem med straffrättsliga påföljder (GrUU 14/2013 rd, GrUU 17/2012 rd, GrUU 9/2012 rd, s. 2/I, GrUU 55/2005 rd, s. 2/I och GrUU 32/2005 rd, s. 2/II). Grundlagsutskottet har konstaterat att trots att den straffrättsliga legalitetsprincipens exaktheskrav inte som sådant kan tillämpas på administrativa påföljder, kan det allmänna kravet på exakthet inte förbigås i samband med reglering av detta slag. Dessutom ska bestämmelserna uppfylla kravet på proportionalitet i fråga om sanktioner (GrUU 37/2021 rd, punkt 32).

Grundlagsutskottet har bedömt ett förslag till motsvarande bestämmelse i samband med AI-förordningen. Utskottet har uppmärksammat att det i AI-förordningen på motsvarande sätt som i den aktuella artikel 53.4 föreslogs att administrativa påföljder kan påföras när andra skyldigheter än säkerhetsrelaterade skyldigheter inte iakttas, vilket verkar innebära att alla slags överträdelser av förordningen är sådana handlingar eller försummelser som kan leda till påföljder. Grundlagsutskottet betraktade det inte i sig som ett förbjudet regleringssätt med tanke på grundlagen, men påpekade att kravet på exakthet och noggrann avgränsning som gäller administrativa påföljdsavgifter inte uppfylls när förordningens bestämmelser om påföljder kan innebära att vilken som helst försummelse, också en partiell, kan bli föremål för en straffavgift, och att en så öppen och oförutsägbar påföljd inte heller framstår som en proportionerlig inskränkning av näringsfriheten (GrUU 37/2021 rd, punkterna 35–36). Förslaget om att påföljdsavgifter för myndigheter är en fråga som får avgöras nationellt är i linje med grundlagsutskottets ståndpunkt. Utskottet har betonat att det bör finnas tillräckligt med nationellt handlingsutrymme i synnerhet med beaktande av att administrativa påföljdsavgifter inte kan påföras myndigheter i Finland, utan myndigheter endast kan påföras straffrättsliga påföljder. (GrUU 37/2021 rd, punkt 40).

6.5 Överföring av förvaltningsuppgifter på andra än myndigheter

De anmälda organens verksamhet är en offentlig förvaltningsuppgift som har överförts på någon annan än en myndighet enligt 124 § i grundlagen. Enligt den paragrafen kan offentliga förvaltningsuppgifter anförtros andra än myndigheter endast genom lag eller med stöd av lag, och endast om det behövs för en ändamålsenlig skötsel av uppgifterna och inte äventyrar de grundläggande fri- och rättigheterna. Uppgifter som innebär betydande utövning av offentlig makt får dock ges endast myndigheter, och endast om det behövs för en ändamålsenlig skötsel av uppgifterna. De organ som anges i förslaget till förordning anförtros myndighetsuppgifter eftersom organen fastställer överensstämmelsen för produkter med digitala element. Denna verksamhet har inte betraktats som betydande utövning av offentlig makt, och myndigheterna har också begränsade möjligheter att sköta en uppgift av den typen, vilket kan leda till att verksamhetens effektivitet lider och utsläppandet på marknaden fördröjs.

När det gäller underleverantörer medger förslaget möjligheten att anlita underleverantörer i bedömningsverksamheten. I en sådan situation ska det anmälda organet försäkra sig om att underleverantören uppfyller kraven på anmälda organ, och underrätta den anmälande myndigheten. Grundlagsutskottet har i princip förhållit sig negativt till sådan subdelegering (GrUU 26/2017 rd), men det har inte rått något absolut förbud mot sådan delegering när det handlar om uppgifter av teknisk natur där samma kvalitetskrav och motsvarande tillsyn gäller både underleverantören och den ursprungliga serviceproducenten (GrUU 6/2013 rd, s. 4).

6.6 Delegering av befogenheter

Det föreslås att befogenheter som gäller förordningens bilagor delegeras till kommissionen. I fråga om bilaga I ska kommissionen kunna anta delegerade akter om underlåtelse att tillämpa kraven i bilagan helt eller delvis. I fråga om bilaga III ska kommissionen kunna anta delegerade akter om innehållet i förteckningen över kritiska produkter. Grundlagsutskottet ansåg i samband med mycket snarlika föreslagna bestämmelser i AI-förordningen att det handlar om eventuell utvidgning av tillämpningsområdet för regleringen, och att bestämmelserna ger kommissionen alltför omfattande befogenheter att ändra förordningen. Enligt artikel 290 i fördraget om Europeiska unionens funktionssätt kan det genom en lagstiftningsakt till kommissionen delegeras befogenhet att anta akter med allmän räckvidd som inte är lagstiftningsakter och som kompletterar eller ändrar vissa icke väsentliga delar av lagstiftningsakten (delegerade rättsakter). Grundlagsutskottet har i detta sammanhang ansett att bestämmelserna behöver preciseras, eftersom ett exakt och noga avgränsat tillämpningsområde för förordningen är av betydelse också för näringsfriheten. (GrUU 37/2021 rd, punkt 41–42).

7 Ålands behörighet

Enligt 27 § 10 punkten i självstyrelselagen för Åland (1144/1991) har riket lagstiftningsbehörighet i fråga om bland annat otillbörligt förfarande i näringsverksamhet, främjande av konkurrens samt konsumentskydd. På grund av att förslaget är av horisontell karaktär tangerar det frågor som också hör till landskapets lagstiftningsbehörighet, eftersom exempelvis informationssystem används som en del av funktionerna i fråga, och de säkerhetskrav som ingår i förslaget därmed också gäller dessa system. Därför är förslaget relevant utifrån 18 § 12–14 och 20–24 punkten i självstyrelselagen.

8 Behandling av förslaget i Europeiska unionens organ och andra medlemsstaters ståndpunkter

Kommissionen antog förslaget till förordning den 15 september 2022.

Behandlingen av förslaget inleddes i rådets övergripande arbetsgrupp för cyberfrågor den 23 september 2022. Inställningen till förslaget har i regel varit positiv.

Behandlingen av förslaget i Europaparlamentet har ännu inte inletts

9 Nationell behandling av förslaget

U-skrivelsen har beretts vid kommunikationsministeriet i samarbete med andra ministerier och ämbetsverk.

Utkastet till U-skrivelse behandlades i sektionen för kommunikation (EU-19) 7.10.2022–12.10.2022 och i sektionen för konkurrenskraft (EU-8) 7.10.2022–12.10.2022. Ett samråd om förslaget ordnades den 23 september 2022.

10 Statsrådets ståndpunkt

Statsrådet understöder den föreslagna förordningens syfte att produkter som släpps ut på marknaden ska vara tryggare i cybermiljön och nivån på säkerhetsegenskaperna hög, samt att säkerhetsegenskaperna och säkerhetskraven ska vara mer transparenta för konsumenter och företag som använder dem. Eftersom den är en horisontell rättsakt kan den föreslagna förordningen konkret förbättra datasäkerheten för alla samhällsaktörer. Statsrådet anser att bättre säkerhet för uppkopplad hårdvara och mjukvara är ett viktigt utvecklingsmål inom cybersäkerhetssektorn. Statsrådet understöder att ansvaret för produktsäkerheten i cybermiljön mer än för närvarande

omriktas från användaren till tillverkaren oavsett var de produkter som släpps ut på den inre marknaden tillverkas. Då mängden uppkopplad hårdvara och mjukvara ökar och deras betydelse accentueras ökar också behovet av att säkerställa deras säkerhet och reagera på eventuella sårbarheter under produktens livscykel.

Statsrådet understöder förordningsförslagets breda tillämpningsområde för att säkerhetskraven på produkter med digitala element ska tillämpas i så stor utsträckning som möjligt på marknaden. För produkter som utnyttjar molntjänster bör man sträva efter att säkerställa att förslaget anger tydliga gränser för ansvar och skyldigheter och är tydligt i förhållande till andra rättsakter som gäller molntjänster, men utan att ge avkall på förslagets syften och utan att utesluta produkter som utnyttjar molnteknik ur förordningens tillämpningsområde. Statsrådet anser att ambitionen under förhandlingarna bör vara att göra förordningens tillämpningsområde så tydligt som möjligt. Statsrådet anser att det är viktigt att den gällande EU-lagstiftningen och den EU-lagstiftning som är under beredning bildar en tydlig och enhetlig helhet så att kraven på olika aktörer är tydliga och proportionerliga, och inte står i strid med de tillämpliga EU-rättsliga kraven. Överlappande bestämmelser bör undvikas och för att minska belastande reglering ska rättsakternas förhållande till varandra vara tydligt. Även förhållandet till exempelvis den föreslagna dataakten, den allmänna dataskyddsförordningen, NIS2-direktivet och CER-direktivet (Critical Entities Resilience Directive) och till kommissionens nyligen antagna förslag om skadeståndsansvar för produkter (COM (2022) 495 final) och skadeståndsansvar gällande AI (COM (2022) 496 final) behöver bedömas närmare under förhandlingarnas gång så att rättsakterna bildar en så integrerad helhet som möjligt.

Statsrådet understöder i princip det riskbaserade tillvägagångssättet för att fastställa krav och skyldigheter. Statsrådet anser att det generellt är bra att särskilja de mest kritiska produkterna med digitala element och låta ett externt anmält organ striktare övervaka att de uppfyller säkerhetskraven. Statsrådet anser dock att det är viktigt att man i förordningen beaktar produkternas huvudsakliga användningsändamål.

De krav som beskrivs i bilagan till förslaget till förordning är enligt statsrådets syn i princip viktiga att beakta i produkter med digitala element. Kravens omfattning och ändamålsenlighet bör bedömas när förhandlingarna går vidare. Statsrådet understöder också det föreslagna kravet att exploaterade sårbarheter ska anmälas för att användarna ska kunna vidta behövliga skyddsåtgärder och informationen om behovet av sådana åtgärder effektivt ska kunna spridas till de aktörer som behöver den. Statsrådet anser att kraven på importörer och distributörer behövs, eftersom deras betydelse framhävs i synnerhet när produkter förs in till den inre marknaden från länder utanför EU eller när tillverkaren upphör med produktionen under produktens livscykel. Statsrådet understöder utgångspunkten att kraven i första hand ställs på tillverkaren och i andra hand på distributören eller importören. I den fortsatta beredningen behöver man också bedöma särskilda skyldigheter vid distansförsäljning och marknadsplatser på nätet samt förslagets förhållande till tillverkare i tredjeländer.

Statsrådet anser att bedömningen av överensstämmelse är väsentlig för att säkerställa att säkerhetskraven uppfylls. Statsrådet anser dock att man i bedömningen av överensstämmelse bör fästa särskild uppmärksamhet vid att undvika överlappningar mellan processer som baseras på olika rättsakter, såsom certifieringar, och vid att utnyttja de befintliga systemen i så hög grad som möjligt. Statsrådet anser att beprövade, befintliga förfaranden behöver tillämpas i så stor utsträckning som möjligt vid bedömningen av överensstämmelse och att nya gemensamma krav bör ställas endast om sådana ännu inte finns. I processen för bedömning av överensstämmelse bör man sträva efter transparens och förutsägbarhet, och processen får inte medföra onödiga olägenheter för EU:s konkurrenskraft och för utsläppandet av ny teknik på marknaden.

När det gäller skyldigheterna att bedöma överensstämmelsen anser statsrådet att det är viktigt att extern bedömning krävs riskbaserat endast för produkter som är särskilt viktiga för cybersäkerheten och att det i regel för andra produkter räcker med tillverkarens interna kontroll. Om behovet av extern bedömning ökar väsentligt och det finns för få sakkunniga bedömningsorgan kan utsläppandet av produkter på marknaden i värsta fall betydligt fördröjas. Statsrådet anser att bedömningen av överensstämmelse bör göras på ett sätt som har faktisk effekt för produktens säkerhetsegenskaper. Statsrådet anser också när det gäller cybersäkerhetskraven att förslaget om CE-märkning är ett bra sätt att visa att produkten överensstämmer med kraven. Det är väsentligt att det tydligt framgår av produkten att den överensstämmer med kraven på cybersäkerhet.

I fråga om kraven på anmälda organ anser statsrådet att det är viktigt att personalens kompetens och tekniska färdigheter är på hög nivå för att nyttan med bedömningarna ska kunna uppnås. Statsrådet anser att det är viktigt för både affärsverksamheten och säkerheten rent allmänt att bedömningsverksamheten är konfidentiell. Statsrådet anser att det är korrekt att de anmälda organen också ansvarar för eventuella underleverantörers verksamhet. Enligt statsrådet är det viktigt att bedömningen utförs effektivt och med iakttagande av proportionalitetsprincipen. Det är viktigt att under förhandlingarna eftersträva att kostnaderna för bedömningen inte blir så höga att det leder till stora problem i synnerhet för små och medelstora företag som vill släppa ut nya produkter på marknaden. Statsrådet anser att det är viktigt att vid beredningen och genomförandet av förslaget ta hänsyn till kostnader och belastande reglering för små och medelstora företag samt behovet av rådgivning vid tillämpningen av kraven. Nationellt gäller det att fästa uppmärksamhet vid att antalet bedömningsorgan är tillräckligt så att bedömningsförfarandet inte onödigt fördröjer utsläppandet av produkterna på marknaden.

Vad gäller marknadskontrollen understöder statsrådet att marknadskontrollförordningen (EU) 2019/1020 tillämpas, med beaktande av att medlemsstaterna får tillräckligt med handlingsutrymme för att utse nationella behöriga myndigheter och ordna marknadskontrollen i praktiken. Statsrådet anser att det är viktigt att kontrollen är förknippad med tillräckliga rättsmedel och att påföljderna för eventuella säkerhetsbrister och bristande överensstämmelse är enhetliga och proportionerliga inom unionens område. Det är också viktigt att de uppgifter och befogenheter som föreslås för dataskyddsmyndigheterna bedöms närmare under förhandlingarna i förhållande till de uppgifter och befogenheter som det föreskrivs om i EU:s allmänna dataskyddsförordning.

När det gäller de befogenheter som enligt förslaget ska delegeras till kommissionen anser statsrådet att behovet och omfattningen av delegerade befogenheter behöver bedömas under förhandlingarnas gång. Statsrådet anser att det är nödvändigt att de befogenheter som delegeras till kommissionen är tydliga, noga avgränsade, proportionerliga, ändamålsenliga och väl motiverade. Förslaget om delegering av lagstiftningsbefogenheter är relevant i synnerhet i förhållande till kraven i samband med extern bedömning, och därför behöver man fästa uppmärksamhet vid möjligheterna att genom delegerade akter utvidga kategorierna av produkter som kräver extern bedömning.

Statsrådet anser att de administrativa påföljder som föreslås i förordningen behövs med beaktande av den ekonomiska nytta som tillverkare, distributörer eller importörer kan ha av att handla svikligt eller i strid med kraven. Statsrådet anser att påföljdernas proportionalitet och rimlighet behöver bedömas under förhandlingarna och att medlemsstaterna bör få tillräckligt med handlingsutrymme att lagstifta om det nationella genomförandet av påföljderna på det sätt som varje medlemsstats rättssystem förutsätter.