EUROPEISKA
KOMMISSIONEN

Strasbourg den 20.1.2026
COM(2026) 13 final

2026/0012 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV

om ändring av direktiv (EU) 2022/2555 vad gäller förenklingsåtgärder och anpassning till [förslag till cybersäkerhetsakt 2]

{SWD(2026) 11-12} - {SEC(2026) 11}

(Text av betydelse för EES)

MOTIVERING

1. BAKGRUND TILL FÖRSLAGET

• Motiv och syfte med förslaget

Detta förslag ingår i ett åtgärdspaket som syftar till att anpassa unionens cybersäkerhetsram till berörda parters behov mot bakgrund av en alltmer sofistikerad cyberhotbild och komplex geopolitisk verklighet. Väsentliga och viktiga entiteter från kritiska sektorer utsätts i allt högre grad för cyberattacker[1], medan statliga fientliga aktörer utnyttjar ny teknik såsom artificiell intelligens (AI) för att ytterligare skala upp och optimera sina attacker. I detta sammanhang erkänns den kritiska infrastrukturens motståndskraft mot cyberhot som en strategisk pelare för våra demokratier och unionens ekonomiska säkerhet. Både EU:s strategi för en beredskapsunion[2] och EU:s strategi för inre säkerhet (ProtectEU)[3] har satt cybersäkerhet i centrum för unionens agenda för resiliens. På samma sätt anges i meddelandet om att stärka EU:s ekonomiska säkerhet[4] att förhindra tillgång till känslig information och känsliga uppgifter som skulle kunna undergräva unionens ekonomiska säkerhet och förebygga och mildra störningar av unionens kritiska infrastruktur som påverkar unionens ekonomi är prioriterade mål, där effektiva cybersäkerhetsåtgärder spelar en avgörande roll. I Draghi-rapporten betonades dessutom behovet av att öka säkerheten och minska beroendet som ett viktigt åtgärdsområde i unionen[5]. I kommissionens meddelande om ett enklare och snabbare Europa[6] tillkännagav kommissionen sitt stöd för ett ambitiöst program för att främja framåtblickande och innovativ politik som stärker unionens konkurrenskraft och minskar regelbördan för allmänheten, företag och förvaltningar samtidigt som höga standarder upprätthålls i fråga om att främja EU:s värden.

Mot den bakgrunden syftar detta förslag till direktiv om ändring av direktiv (EU) 2022/2555 vad gäller förenklingsåtgärder och anpassning till [förslaget till Europaparlamentets och rådets förordning om Europeiska unionens cybersäkerhetsbyrå (Enisa), den europeiska ramen för cybersäkerhetscertifiering och säkerhet i IKT-leveranskedjan och om upphävande av förordning (EU) 2019/881 (cybersäkerhetsakten 2)] till att gripa sig an problemet med komplexiteten och mångfalden i den cybersäkerhetsrelaterade politik som påverkar unionens cybersäkerhetsstatus, särskilt genom att införa förtydliganden och underlätta efterlevnaden för de reglerade entiteterna.

Syftet med detta direktiv bör betraktas som en del av de övergripande målen för paketet för översyn av cybersäkerhetsakten som inbegriper förslaget till Europaparlamentets och rådets förordning om Europeiska unionens cybersäkerhetsbyrå (Enisa), den europeiska ramen för cybersäkerhetscertifiering och säkerhet i IKT-leveranskedjan och om upphävande av förordning (EU) 2019/881. Förslaget till förordning syftar till att åtgärda följande: i) Den bristande överensstämmelsen mellan unionens policyram för cybersäkerhet och intressenternas behov i en alltmer fientlig hotbild. ii) Det avstannade genomförandet av det europeiska ramverket för cybersäkerhetscertifiering (ECCF). iii) Komplexiteten och

---

1 ENISA, ENISA Threat Landscape 2025.
2 JOIN/2025/130 final.
3 COM/2025/148 final.
4 JOIN(2025) 977 final.
5 Europeiska kommissionen, *Rapport om EU:s framtida konkurrenskraft*, https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf.
6 COM(2025) 47 final.

mångfalden hos den cybersäkerhetsrelaterade politiken som påverkar unionens cybersäkerhetsstatus. iv) öka säkerhetsriskerna i IKT-leveranskedjorna. När det gäller komplexiteten och mångfalden i den cybersäkerhetsrelaterade politik som påverkar unionens cybersäkerhetsstatus föreslås i översynspaketet för cybersäkerhetsakten – som en del av en reform av den europeiska ramen för cybersäkerhetscertifiering – att man ska främja certifiering som ett efterlevnadsverktyg för företag och göra det möjligt att utveckla ett system för entiteters cybersäkerhetsstatus för att minska efterlevnadskostnaderna för entiteter som omfattas av NIS 2-direktivet och annan relevant unionslagstiftning om cybersäkerhet. Detta tillvägagångssätt kommer att avsevärt förenkla de lagstadgade skyldigheterna för enheter som omfattas av flera efterlevnadskrav och säkerställa en effektivare resursanvändning av alla nationella myndigheter.

I motiveringen till förslaget till förordning om cybersäkerhetsakt 2 beskrivs de viktigaste frågor som ligger till grund för förslaget samt de specifika målen för att hantera dem. Förslaget till direktiv kommer att behandla det särskilda målet nr 4 i konsekvensbedömningen för översynen av cybersäkerhetsakten, nämligen att fastställa mekanismer och villkor för att underlätta efterlevnaden av cybersäkerhetskraven och därigenom göra genomförandet av dem mer konsekvent och effektivt. Riktade ändringar av NIS 2-direktivet syftar till att förenkla efterlevnaden av och säkerställa ett anpassat och enhetligt genomförande av specifika aspekter av cybersäkerhetsramen, bland annat när det gäller tillämpningsområde, definitioner, rapportering av utpressningsprogram och tillsyn över entiteter som tillhandahåller gränsöverskridande tjänster.

Förslaget till direktiv om ändring av direktiv (EU) 2022/2555 om förenklingsåtgärder och anpassning till [cybersäkerhetsakten 2] omfattas av programmet om lagstiftningens ändamålsenlighet och resultat (Refit-programmet). Tillsammans med översynen av cybersäkerhetsakten bidrar det i hög grad till att förbättra tydligheten, minska ineffektiviteten och anpassa förfarandena mellan olika rättsliga ramar. Det bidrar till en väl fungerande inre marknad och säkerställer samtidigt unionens säkerhet och strategiska oberoende.

- **Förenlighet med befintliga bestämmelser inom området**

Unionen har utökat sina rättsliga och politiska verktyg genom att anta ett antal rättsliga instrument och politiska åtgärder: i) NIS 2-direktivet som syftar till att stärka cybersäkerheten för kritisk infrastruktur. ii) Fysiska säkerhetsåtgärder, såsom definieras i dess systerdirektiv, direktivet om kritiska entiteters motståndskraft (CER-direktivet). iii) Cyberresiliensförordningen som förbättrar cybersäkerheten för produkter. iv) Cybersolidaritetsakten som bygger upp EU-omfattande insatskapacitet. v) EU:s cyberplan[7] som stöder krishanteringssamarbete på EU-nivå. vi) EU:s verktygslåda för 5G-säkerhet som stöder cybersäkerhet i 5G-nät. vii) Den europeiska handlingsplanen för cybersäkerhet för sjukhus och vårdgivare[8], som bidrar till att förbättra deras cybersäkerhet. och viii) EU-akademin för cyberkompetens[9] som behandlar den ökande kompetensbristen på cybersäkerhetsområdet.

Ovannämnda rättsliga ramverk för cybersäkerhet kompletterades med sektorsspecifik lagstiftning, nämligen förordningen om digital operativ motståndskraft (DORA-förordningen) för finanssektorn, nätföreskriften om sektorsspecifika regler för cybersäkerhetsaspekter av

7 COM/2025/66 final.
8 COM(2025) 10 final.
9 COM(2023) 207 final.

gränsöverskridande elflöden (NCCS) för delsektorn för elektricitet, informationssäkerhetsregler (Del-IS[10]) för delsektorn för lufttransporter.

Detta förslag till direktiv är, i likhet med det förslag till förordning som det åtföljer, en del av en bredare uppsättning rättsliga och politiska initiativ som antagits av unionen för att förbättra entiteternas motståndskraft mot säkerhets- och cyberhot. Det är inriktat på riktade ändringar av NIS 2-direktivet som bland annat syftar till att klargöra vissa aspekter när det gäller tillämpningsområde, definitioner och behörighetsregler, minska bördan vid tillsynen av väsentliga och viktiga entiteter och underlätta tillsynen av gränsöverskridande entiteter genom att stärka Enisas roll i stödet till operativt samarbete. Tillsammans med förslaget till förordning skapar detta förslag dessutom en stark synergi som härrör från utvecklingen av certifiering av cybersäkerhetsstatus för NIS 2-direktivet samt potentiellt för att underlätta efterlevnaden av andra relevanta unionsrättsakter, såsom den allmänna dataskyddsförordningen, utan att det påverkar deras särskilda certifieringskrav. Dessa förenklingsåtgärder bör frigöra resurser för att stärka den operativa cybersäkerhetsberedskapen hos entiteter i unionens kritiska sektorer.

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

Detta förslag skärper säkerhetskraven för de entiteter som tillhandahåller företagsplånböcker i enlighet med förslaget till Europaparlamentets och rådets förordning om inrättande av europeiska företagsplånböcker.[11] Dessutom kommer kommissionen att säkerställa överensstämmelse med kommande initiativ, såsom rättsakten om digitala nätverk. Detta förslag är i linje med förslaget till förordning om förenkling av den digitala lagstiftningen (det digitala omnibuspaketet), som bland annat innehåller ändringar av NIS 2-direktivet, tillsammans med andra unionsrättsakter. I det digitala omnibuspaketet föreslås att efterlevnaden av rapporteringskraven för cybersäkerhet ska ändras, bland annat enligt NIS 2-direktivet, genom rapportering via en gemensam kontaktpunkt för incidentrapportering, som ska utvecklas och underhållas av Enisa. Dessutom är detta förslag i linje med förslaget till Europaparlamentets och rådets förordning om säkerhet, resiliens och hållbarhet i rymdverksamhet i unionen[12].

Dessutom är förslaget i linje med Mario Draghis rapport om den europeiska konkurrenskraftens framtid, såsom framhålls ovan.

2. RÄTTSLIG GRUND, SUBSIDIARITETSPRINCIPEN OCH PROPORTIONALITETSPRINCIPEN

- **Rättslig grund**

Den rättsliga grunden för detta förslag är artikel 114 i fördraget om Europeiska unionens funktionssätt, vars mål är att upprätta den inre marknaden och säkerställa dess funktion genom att förbättra åtgärderna för tillnärmning av nationella regler. Genom detta förslag ändras direktiv (EU) 2022/2555, som antogs i enlighet med artikel 114 i EUF-fördraget.

[10] Kommissionens genomförandeförordning (EU) 2023/203 och kommissionens delegerade förordning (EU) 2022/1645.

[11] COM/2025/838 final.

[12] COM/2025/335 final.

- **Subsidiaritetsprincipen (för icke-exklusiv befogenhet)**

Subsidiaritetsprincipen kräver att det görs en bedömning av nödvändigheten och mervärdet av en åtgärd på unionsnivå. Förenligheten med subsidiaritetsprincipen på detta område erkändes redan vid antagandet av direktiv (EU) 2022/2555, som ändras genom detta förslag.

Detta förslag underlättar efterlevnaden av unionens cybersäkerhetslagstiftning, minskar efterlevnadskostnaderna och den rättsliga osäkerheten för berörda entiteter samt underlättar och förbättrar efterlevnaden av cybersäkerhetskraven. Det bidrar också till att skapa lika villkor när det gäller metoder för tillsyn och efterlevnadskontroller i medlemsstaterna.

- **Proportionalitet**

De regler som föreslås i detta direktiv går inte utöver vad som är nödvändigt för att i tillräckligt hög grad uppnå de särskilda målen. Den planerade anpassningen och rationaliseringen av tillämpningsområde, säkerhetsåtgärder och rapporteringsskyldigheter har samband med medlemsstaternas och företagens önskemål om en förbättring av den nuvarande ramen.

- **Val av instrument**

Förslaget kommer att ändra det befintliga NIS 2-direktivet och ytterligare rationalisera de skyldigheter som åläggs företag, och därmed säkerställa en högre harmoniseringsnivå i hela unionen. Valet av rättsligt instrument för detta förslag är förenligt med valet av den rättsakt som det ändrar, dvs. NIS 2-direktivet. Detta förslag bygger på syftet med NIS 2-direktivet att ge medlemsstaterna den flexibilitet som krävs för att ta hänsyn till nationella särdrag.

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

- **Efterhandsutvärderingar/kontroller av ändamålsenligheten med befintlig lagstiftning**

Se motiveringen till [förslag till cybersäkerhetsakt 2].

- **Samråd med berörda parter**

Se motiveringen till [förslag till cybersäkerhetsakt 2].

- **Insamling och användning av sakkunnigutlåtanden**

Se motiveringen till [förslag till cybersäkerhetsakt 2].

- **Konsekvensbedömning**

Se motiveringen och den konsekvensbedömning som åtföljer [förslag till cybersäkerhetsakt 2].

- **Lagstiftningens ändamålsenlighet och förenkling**

Se motiveringen till [förslag till cybersäkerhetsakt 2].

- **Grundläggande rättigheter**

Se motiveringen till [förslag till cybersäkerhetsakt 2].

4. BUDGETKONSEKVENSER

Se lagstiftnings- och finansieringsöversikten i [förslag till cybersäkerhetsakt 2].

5. ÖVRIGA INSLAG

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

Enligt artikel 40 i NIS 2-direktivet ska kommissionen se över hur direktivet fungerar och rapportera resultatet till Europaparlamentet och rådet var 36:e månad.

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

Förslaget syftar till att underlätta efterlevnaden av cybersäkerhetsskyldigheter och frigöra resurser för att stärka den operativa cybersäkerhetsberedskapen hos entiteter inom unionens kritiska sektorer.

Genom förslaget införs riktade ändringar av NIS 2-direktivet för att förenkla specifika aspekter av cybersäkerhetsramen, öka rättssäkerheten och harmonisera genomförandet.

För att göra det lättare för entiteter och leverantörer att visa efterlevnad av NIS 2-direktivet, i linje med det förslag till förordning som detta förslag åtföljer, kommer entiteter som regleras av NIS 2-direktivet att kunna erhålla certifikat inom ramen för organisatoriska system för cybersäkerhetscertifiering som utvecklats inom det europeiska ramverket för cybersäkerhetscertifiering.

För att ytterligare underlätta efterlevnaden av riskhanteringsåtgärder för cybersäkerhet för entiteter som omfattar flera länder och som står under tillsyn av behöriga myndigheter från flera medlemsstater har Enisa fått en ny roll som stöder medlemsstaterna i tillsynen av dessa entiteter, underlättar ömsesidigt bistånd och skapar en bättre överblick över de entiteter som omfattas av NIS 2-direktivet.

Enligt förslaget ska kommissionen dessutom anta riktlinjer för tillämpningen av de säkerhetskrav i leveranskedjan som entiteter som omfattas av NIS 2-direktivet överför till sina leverantörer, i syfte att säkerställa rättssäkerhet och förhindra otillbörlig övervältring av skyldigheter på entiteter som inte omfattas av NIS 2-direktivet.

Andra riktade ändringar av NIS 2-direktivet är följande:

- Förtydligande av tillämpningsområde och definitioner.
- Strykning av leverantörer av DNS-tjänster som är mikroföretag eller små företag från tillämpningsområdet.
- Införande av maximal harmonisering för genomförandeakter enligt artikel 21.5 (som specificerar riskhanteringsåtgärder för cybersäkerhet) för att underlätta entiteternas efterlevnad och myndigheternas tillsyn.
- Införande av en ny kategori av små midcapföretag, i linje med 2025 års kommissionsrekommendation om definition av små midcapföretag[18]. Enheter som klassificeras som små midcapföretag ska betecknas som viktiga entiteter, vilket minskar deras efterlevnadsbörda och tillsynsbördan för de behöriga myndigheterna.
- Kravet på att medlemsstaterna ska anta strategier för migrering till postkvantkryptografi (PQC) som en del av sin nationella strategi för cybersäkerhet.
- Införande av en harmoniserad insamling av uppgifter om attacker med utpressningsprogram.

2026/0012 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV

om ändring av direktiv (EU) 2022/2555 vad gäller förenklingsåtgärder och anpassning till [förslag till cybersäkerhetsakt 2]

(Text av betydelse för EES)

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DETTA DIREKTIV

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) I Europaparlamentets och rådets direktiv (EU) 2022/2555[3] fastställs åtgärder för att uppnå en hög gemensam cybersäkerhetsnivå inom unionen, i syfte att förbättra den inre marknadens funktion. Sedan direktiv (EU) 2022/2555 trädde i kraft har framsteg gjorts med att öka unionens nivå av cyberresiliens. Samtidigt har vissa utmaningar uppstått under medlemsstaternas genomförande, bland annat när det gäller direktivets tillämpningsområde, genomförandet av riskhanterings- och incidentrapporteringsskyldigheterna för cybersäkerhet och tillsynen över gränsöverskridande entiteter. Med utgångspunkt i [förslag till cybersäkerhetsakt 2] bör riktade ändringar göras av direktiv (EU) 2022/2555 för att möta dessa utmaningar, genom att förenkla specifika aspekter i syfte att öka rättssäkerheten och säkerställa ett enhetligt genomförande av direktiv (EU) 2022/2555.

(2) För att minska efterlevnadsbördan för entiterna och tillsynsbördan för de behöriga myndigheterna bör en ny kategori av små midcapföretag införas i direktiv (EU) 2022/2555, i linje med kommissionens rekommendation (EU) 2025/1099[4]. Entiteter av den typ som avses i bilaga I till direktiv (EU) 2022/2555, som klassificeras som små midcapföretag enligt den rekommendationen, bör som huvudregel betecknas viktiga

---

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

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

3 Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet) (EUT L 333, 27.12.2022, s. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

4 Kommissionens rekommendation (EU) 2025/1099 av den 21 maj 2025 om definition av små midcapföretag (EUT L, 2025/1099, 28.5.2025, ELI: http://data.europa.eu/eli/reco/2025/1099/oj).

entiteter. För att stödja kommissionens mål att minska de administrativa kostnaderna med totalt 25 % och med 35 % för de små och medelstora företagen bör dessutom den allmänna storleksbegränsningsregel som föreskrivs i direktiv (EU) 2022/2555, enligt vilken alla enheter som räknas som medelstora företag enligt artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG[5], eller överskrider de tak för medelstora företag som föreskrivs i punkt 1 i den artikeln, omfattas av direktiv (EU) 2022/2555, tillämpas på leverantörer av domännamnssystemtjänster.

(3) Under genomförandet av direktiv (EU) 2022/2555 har det förekommit utmaningar när det gäller tolkningen av bestämmelserna om dess tillämpningsområde. Därför bör vissa tillämpningsrelaterade bestämmelser som avser vårdgivare, elproducenter, vätgasföretag och entiteter inom den kemiska sektorn förtydligas för att säkerställa rättssäkerheten och minska efterlevnadsbördan för både entiteterna och de nationella myndigheterna.

(4) För att säkerställa proportionaliteten i fråga om elproducenter enligt artikel 2.38 i Europaparlamentets och rådets direktiv (EU) 2019/944[6] bör endast de elproducenter som har en total produktionskapacitet på mer än 1 MW anses vara väsentliga eller viktiga entiteter enligt direktiv (EU) 2022/2555, förutsatt att de uppfyller storleksbegränsningsregeln. Detta bör omfatta elproducenter med en enda elproduktionsanläggning som överstiger 1 MW och elproducenter som driver flera produktionsanläggningar som tillsammans har en produktionskapacitet som överstiger 1 MW. Ett sådant tillvägagångssätt möjliggör en balans mellan behovet av att fånga upp de enheter där störningar i deras nätverks- och informationssystem skulle kunna medföra en förlust, okontrollerbarhet eller extern kontroll av produktionskapaciteten som i sig är relevant för elnätets säkerhet och stabilitet, och behovet av att inte lägga en oproportionerlig administrativ börda på företag enligt direktiv (EU) 2022/2555.

(5) De europeiska digitala identitetsplånböckerna, som föreskrivs i Europaparlamentets och rådets förordning (EU) nr 910/2014[7], är en väsentlig del av unionens digitala infrastruktur och möjliggör säker identifiering och autentisering samt utbyte av elektroniska dokument, inbegripet elektroniska attributsintyg. Med tanke på deras avgörande roll för allmänheten och för tillhandahållandet av offentliga och privata tjänster skulle alla cybersäkerhetsincidenter som påverkar dessa plånböcker kunna ha en bred inverkan. För att tillhandahållandet av de tjänster som tillhandahållarna av europeiska digitala identitetsplånböcker tillhandahåller ska säkerställas bör de vara skyldiga att genomföra lämpliga tekniska, operativa och organisatoriska åtgärder för att hantera cybersäkerhetsrisker, förebygga och hantera incidenter och samarbeta med behöriga myndigheter i enlighet med direktiv (EU) 2022/2555. De bör därför ingå bland de entiteter som omfattas av det direktivet oavsett deras storlek och klassificeras som väsentliga entiteter. De europeiska företagsplånböckerna erbjuder liknande funktioner och tjänster som är anpassade till de ekonomiska aktörernas och de

---

5 Kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag (EUT L 124, 20.5.2003, s. 36, ELI: http://data.europa.eu/eli/reco/2003/361/oj).

6 Europaparlamentets och rådets direktiv (EU) 2019/944 av den 5 juni 2019 om gemensamma regler för den inre marknaden för el och om ändring av direktiv 2012/27/EU (EUT L 158, 14.6.2019, s. 125, ELI: http://data.europa.eu/eli/dir/2019/944/oj).

7 Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (EUT L 257, 28.8.2014, s. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

offentliga myndigheternas behov, med utgångspunkt i EU:s ramverk för digital identitet, och är lika kritiska för den digitala ekonomins säkerhet och integritet. Följaktligen bör tillhandahållarna av europeiska företagsplånböcker, som inrättas i enlighet med[förslag till förordning om inrättande av europeiska företagsplånböcker][8], omfattas av samma cybersäkerhetskrav och cybersäkerhetsskyldigheter som tillhandahållarna av europeiska digitala identitetsplånböcker, för att säkerställa en konsekvent och hög säkerhetsnivå i hela ekosystemet för digital identitet.

(6) Infrastruktur för dataöverföring under vatten omfattar inte bara kablar utan även infrastruktur som hänför sig till driften av dem. Sådan infrastruktur omfattar markstationer och undervattenskabelns anslutningsdelar ovan mark (till exempel landvägar från inspektionsbrunnen på stranden till en markstation, datacentral eller ”point of presence”). Infrastruktur för dataöverföring under vatten drivs vanligtvis av enheter som redan omfattas av direktiv (EU) 2022/2555, inbegripet leverantörer av allmänna elektroniska kommunikationsnät och kommunikationstjänster eller leverantörer av molntjänster. Infrastrukturen för dataöverföring under vatten kan dock också drivas av andra typer av entiteter som för närvarande inte omfattas av direktiv (EU) 2022/2555, såsom infrastruktur för dataöverföring under vatten som drivs av leverantörer av elektroniska kommunikationsnät som inte är allmänna, eller av entiteter som leasar driften av infrastruktur för dataöverföring under vatten antingen helt eller delvis till leverantörer av allmänna elektroniska kommunikationsnät. Med tanke på de ökande riskerna för infrastruktur för dataöverföring under vatten och den därav följande höga kritikaliteten är det nödvändigt att säkerställa att alla typer av operatörer av infrastruktur för dataöverföring under vatten omfattas av direktiv (EU) 2022/2555. Annan havsbaserad kritisk infrastruktur, såsom elkablar under vattnet samt gas-, vätgas- och oljeledningar, omfattas normalt redan av direktiv (EU) 2022/2555, eftersom de drivs av systemansvariga för överföringssystem inom delsektorerna el, gas, vätgas och olja.

(7) För att göra det möjligt för de entiteter som tillhandahåller tjänster i flera medlemsstater att dra nytta av mer enhetliga och mindre betungande tillsynsmetoder på hela den inre marknaden bör de entiteterna kunna visa att de uppfyller specifika eller samtliga skyldigheter avseende hantering av cybersäkerhetsrisker som fastställs i direktiv (EU) 2022/2555 genom att beviljas ett certifikat om cybersäkerhetsstatus inom ramen för en europeisk ordning för cybersäkerhetscertifiering. Utvecklingen av en sådan ordning kommer att gynnas av antagandet av genomförandeakter om tekniska och metodologiska krav samt de sektorsspecifika krav avseende riskhanteringsåtgärder för cybersäkerhet som föreskrivs i direktiv (EU) 2022/2555 och som bygger på maximal harmonisering.

(8) Med tanke på vårt samhälles och vår ekonomis ständigt ökande beroende av digital teknik är det nödvändigt att vidta begränsningsåtgärder mot kvanthotet. Möjligheten av ”lagra nu, dekryptera senare”-attacker (*harvest now - decrypt later*), som sannolikt pågår redan i dag, och den framtida risken för kvantattacker till följd av förfalskning av namnteckningar, liksom den avskrivning av vissa bestämda algoritmtillämpningar och det fullständiga borttagande av aktuella krypteringsalgoritmer med öppna nycklar som planeras, gör behovet av att inleda åtgärder för att migrera till postkvantkryptografi (PQC) desto mer brådskande. Medlemsstaterna bör därför vara skyldiga att anta strategier för att migrera till PQC som en del av sina nationella

[8] COM(2025) 838 final.

strategier för cybersäkerhet. De strategierna bör göra det lättare att påskynda strategisk planering och att skapa stödåtgärder och verktyg för att bedöma krypteringsresursers exponering för de risker som kvantdatorerna medför. De bör dessutom bidra till att skapa en migrationsplan och testa införandet av PQC i digitala tillämpningar och nätverk, och samtidigt främja framväxten och användningen av formellt verifierade och utvärderade europeiska PQC-lösningar som följer efterlevnadsramverket för produkter och tjänster. De strategierna bör anpassas till de delmål som fastställs i unionens rättsakter och politik och till de dokument som antagits av samarbetsgruppen för nät- och informationssäkerhet, särskilt den samordnade färdplanen för genomförandet av övergången till PQC, som antogs av samarbetsgruppen för nät- och informationssäkerhet i juni 2025, som på så sätt fullbordar migrationen till PC senast 2030 för kritiska användningsfall, och senast 2035 för användningsfall med medelhög och låg nivå.

(9) Enligt artikel 21.2 d i direktiv (EU) 2022/2555 ska de väsentliga och viktiga entiteterna säkerställa en lämplig säkerhetsnivå i sin leveranskedja. I praktiken har denna skyldighet lett till att många enheter har begärt omfattande information från sina leverantörer med hjälp av heterogena frågeformulär, format och processer. Även om sådana begäranden syftar till att stödja tillbörlig aktsamhet och riskhantering kan de skapa en betydande administrativ börda för leverantörer till väsentliga och viktiga entiteter, särskilt när liknande information måste tillhandahållas upprepade gånger i olika former. För att minska denna börda och främja en konsekvent, proportionell och effektiv strategi för säkerhetsbedömningar i leveranskedjan bör kommissionen utarbeta riktlinjer för att rekommendera passande detaljnivå, struktur och format för sådana begäranden om information. Riktlinjerna bör underlätta harmonisering, minska onödigt dubbelarbete och hjälpa både entiteter och deras leverantörer att effektivt fullgöra sina skyldigheter enligt direktiv (EU) 2022/2555.

(10) Attacker med utpressningsprogram i vilka sabotageprogram krypterar uppgifter och system och kräver en lösensumma för frigörande är fortfarande ett av de främsta hoten mot väsentliga och viktiga entiteter. En harmonisering och förbättring av insamlingen av uppgifter om attacker med utpressningsprogram från de berörda väsentliga och viktiga entiteter skulle ge enheterna för hantering av it-säkerhetsincidenter (CSIRT-enheterna) och de nationella myndigheterna insikter som gör att de kan säkerställa att framtida ingripanden avseende utpressningsprogram är lämpliga och effektiva, hjälpa entiteter att öka sin motståndskraft och förhindra framtida attacker, och sammanställa de underrättelser och bevis som de brottsbekämpande organen behöver för att störa och upplösa gäng med utpressningsprogram och bestraffa sina anställda. Med tanke på den potentiellt känsliga karaktären hos den information som ska utbytas om attacker med utpressningsprogram, särskilt huruvida en enhet har betalat en lösensumma, och i så fall vilket belopp och till vem, bör sådan information endast lämnas till CSIRT-enheter eller, i tillämpliga fall, behöriga myndigheter på deras begäran. För sådant informationsutbyte uppmuntras väsentliga och viktiga entiteter att utse en person som fungerar som kontaktpunkt och säkerställer informationsutbytets konfidentialitet och tillförlitlighet. Inom ramen för det internationella initiativet för att motverka utpressningsprogram har unionen godkänt en icke-bindande internationell policyförklaring enligt vilken relevanta institutioner under de deltagande nationella regeringarnas överinseende inte bör betala det belopp som krävs av utpressningsprogram.

(11) Fullgörandet av skyldigheterna att rapportera relevant information om incidenter med utpressningsprogram bör inte leda till införandet av några ytterligare skyldigheter

enligt direktiv (EU) 2022/2555 som entiteten inte skulle ha varit föremål för om den inte hade rapporterat informationen. I detta syfte bör medlemsstaterna, inom ramen för sin nationella rättsordning, hantera eventuella risker som uppstår till följd av ökat ansvar i samband med rapportering av relevant information om incidenter med utpressningsprogram.

(12) Med tanke på den gränsöverskridande dimensionen hos många väsentliga och viktiga entiteter på hela den inre marknaden och behovet av att säkerställa samstämmighet och främja konvergens och effektivitet när det gäller tillsynsmetoder, bör Enisa stödja medlemsstaterna i genomförandet av ömsesidigt bistånd för väsentliga och viktiga entiteter som tillhandahåller tjänster i mer än en medlemsstat eller som tillhandahåller tjänster i en eller flera medlemsstater och vars nätverks- och informationssystem är belägna i en eller flera andra medlemsstater. För detta bör medlemsstaterna lämna in ytterligare information till Enisas register över entiteter. På grundval av informationen i registret över väsentliga och viktiga entiteter bör Enisa genomföra en omfattande analys av gränsöverskridande cybersäkerhetsrisker som rör väsentliga och viktiga entiteter. Analysen bör baseras på en metod som utvecklats tillsammans med kommissionen och samarbetsgruppen för nät- och informationssäkerhet. Denna metod skulle kunna ta hänsyn till i vilken utsträckning väsentliga och viktiga entiteter använder sina tjänster över gränserna, är beroende av gränsöverskridande tjänster, är utsatta för en koncentrationsrisk i leveranskedjan, kan identifieras som en källa till koncentrationsrisk i leveranskedjan, är utsatta för incidenter som skulle kunna ha betydande störande effekter på gränsöverskridande tjänster eller är beroende av nätverks- och informationssystem för tillhandahållandet av sina tjänster som är belägna i olika medlemsstater och utanför unionen. På grundval av riskanalysrapporten bör Enisa rekommendera de relevanta behöriga myndigheterna att inrätta gemensamma undersökningsgrupper för att stödja tillsynen av entiteter med en högre risknivå för en väl fungerande inre marknad i händelse av incidenter och bistå de behöriga myndigheterna i genomförandet av gemensamma tillsynsåtgärder på deras begäran.

(13) Eftersom målet för detta direktiv, nämligen att uppnå en hög gemensam cybersäkerhetsnivå i unionen, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare, på grund av åtgärdens verkningar, kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen. I enlighet med proportionalitetsprincipen i samma artikel går detta direktiv inte utöver vad som är nödvändigt för att uppnå detta mål.

(14) Europeiska datatillsynsmannen och Europeiska dataskyddsstyrelsen har hörts i enlighet med artikel 42 i Europaparlamentets och rådets förordning[9] (EU) 2018/1725 och avgav ett gemensamt yttrande den 31 mars 2021.

[9] Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

HÄRIGENOM F<ÖRESKRIVS FÖLJANDE.

Artikel 1

Ändringar av direktiv (EU) 2022/2555

Direktiv (EU) 2022/2555 ska ändras på följande sätt:

(1) Artikel 2 ska ändras på följande sätt:

(a) I punkt 2 ska led a ändras på följande sätt:

i) Led iii ska ersättas med följande:

”iii) registreringsenheter för toppdomäner,”

ii) Följande led ska läggas till som leden iv och v:

”tillhandahållare av europeiska digitala identitetsplånböcker i enlighet med förordning (EU) nr 910/2014,”

v) tillhandahållare av europeiska företagsplånböcker som inrättats i enlighet med förordning (EU) [...]*.

_____

* ”Förordning (EU) [...] [förslag till förordning om inrättande av europeiska företagsplånböcker].”

(b) Följande punkt ska införas som punkt 3a:

”3a. Detta direktiv är tillämpligt på entiteter som identifieras som ägare, förvaltare och operatörer av strategisk infrastruktur med dubbla användningsområden enligt förordning (EU) [...] **, oavsett storlek.

_____

** ”[...] förordning (EU) [...] [Förslag till Europaparlamentets och rådets förordning om inrättande av en åtgärdsram för att underlätta transport av militär utrustning, militära varor och militär personal i hela unionen].”

(2) Artikel 3 ska ändras på följande sätt:

(a) Punkt 1 ska ändras på följande sätt:

i) Leden a och b ska ersättas med följande:

”a) Entiteter av en typ som avses i bilaga I som överstiger trösklarna för små midcapföretag.

b) Kvalificerade tillhandahållare av betrodda tjänster, tillhandahållare av europeiska digitala identitetsplånböcker, tillhandahållare av europeiska företagsplånböcker och registreringsenheter för toppdomäner, oavsett storlek.”.

Följande led ska läggas till som led h:

”h) Entiteter som identifieras som ägare, förvaltare och operatörer av strategisk infrastruktur med dubbla användningsområden enligt förordning (EU) [...] [Förslag till Europaparlamentets och rådets förordning om inrättande av en åtgärdsram för att underlätta transport av militär utrustning, militära varor och militär personal i hela unionen].”

(b) I punkt 4 ska första stycket ersättas med följande:

”Vid upprättandet av den förteckning som avses i punkt 3 ska medlemsstaterna ålägga de entiteter som avses i den punkten att lämna minst följande information till de behöriga myndigheterna:

a) Entitetens namn.

b) Den relevanta sektorn och delsektorn samt typen av entitet enligt bilaga I eller II i tillämpliga fall.

c) Entitetens adress eller, i tillämpliga fall, adressen till entitetens huvudsakliga etableringsställe och andra rättsligt giltiga etableringsställen i unionen eller, om entiteten inte är etablerad i unionen, till dess företrädare som utsetts i enlighet med artikel 26.3.

d) Entitetens aktuella kontaktuppgifter, inklusive e-postadresser, telefonnummer, och den unika identifikationskoden och de digitala adresserna för entitetens europeiska företagsplånbok, i tillämpliga fall, och entitetens företrädare som utsetts i enlighet med artikel 26.3, i tillämpliga fall.

e) De medlemsstater där entiteten tillhandahåller tjänster.

f) Entitetens IP-adressintervall.

(3) Artikel 5 ska ersättas med följande:

”*Artikel 5*

Minimiharmonisering

Utan att tillämpningen av artikel 21.5 femte stycket påverkas hindrar detta direktiv inte medlemsstaterna från att anta eller behålla bestämmelser som säkerställer en högre cybersäkerhetsnivå, förutsatt att sådana bestämmelser står i överensstämmelse med medlemsstaternas förpliktelser enligt unionsrätten.”

(4) I artikel 6

ska följande punkter läggas till som punkterna 42 och 43:

”42. *små midcapföretag*: små midcapföretag enligt definitionen i bilagan till kommissionens rekommendation (EU) 2025/1099***.

43. *infrastruktur för dataöverföring under vatten*: undervattenskablar som överför data, tillhörande infrastruktur och andra anläggningar eller element som är kopplade till dataöverföring.

_____

*** Kommissionens rekommendation (EU) 2025/1099 av den 21 maj 2025 om definition av små midcapföretag (EUT L, 2025/1099, 28.5.2025, ELI: http://data.europa.eu/eli/reco/2025/1099/oj).”

(5) I artikel 7.2 ska följande led läggas till som led k:

”k) Riktlinjer för övergången till postkvantkryptografi, med beaktande av de tidsramar för övergången och relevanta krav som fastställs i unionens tillämpliga rättsakter och politik.”

(6) I artikel 15.2 ska den första meningen ersättas med följande:

”CSIRT-nätverket ska bestå av företrädare för de CSIRT-enheter som utsetts eller inrättats i enlighet med artikel 10, incidenthanteringsorganisationen för unionens institutioner, organ och byråer (Cert-EU) och Enisa.”

(7) Artikel 21.5 ska ändras på följande sätt:

(a) Andra stycket ska ersättas med följande:

”Kommissionen får anta genomförandeakter för att fastställa tekniska och metodologiska krav samt, vid behov, sektorskrav för de åtgärder som avses i punkt 2 med avseende på andra väsentliga och viktiga entiteter än de som avses i första stycket i denna punkt. Kommissionen ska regelbundet bedöma huruvida de genomförandeakter som avses i detta stycke ska antas för specifika sektorer eller typer av entiteter för att förbättra den inre marknadens funktion. När kommissionen utarbetar sådana bedömningar ska den särskilt fokusera på sektorers eller entitetstypers gränsöverskridande karaktär och genomföra en öppen, transparent och inkluderande samrådsprocess med de berörda parterna och medlemsstaterna.”

(b) Följande stycke ska läggas till som femte stycke:

”Om kommissionen antar sådana genomförandeakter som avses i första och andra stycket i denna punkt, får medlemsstaterna inte införa några ytterligare tekniska krav, metodologiska krav eller sektorskrav för de åtgärder som avses i artikel 21.2 i direktiv (EU) 2022/2555 för de entiteter som omfattas av de genomförandeakterna.”

(8) I artikel 23 ska följande punkter läggas till som punkterna 12 och 13:

”12. När kommissionen antar en genomförandeakt i enlighet med punkt 11 första stycket ska den inkludera krav på att följande information avseende attacker med utpressningsprogram lämnas in i enlighet med punkt 1:

(a) Huruvida entiteten upptäckte en attack med utpressningsprogram.

(b) Attackvektorn för attacken med utpressningsprogram.

(c) Huruvida begränsningsåtgärder har vidtagits.

13. Medlemsstaterna ska säkerställa att de berörda entiteterna, i händelse av en betydande incident som orsakas av en attack med utpressningsprogram, på begäran av CSIRT-enheten eller, i tillämpliga fall, den behöriga myndigheten via en kommunikationskanal som tillhandahålls av CSIRT-enheten eller, i tillämpliga fall, den behöriga myndigheten, lämnar in följande information:

(a) Huruvida entiteten har mottagit ett krav på lösensumma och, om så är fallet, från vem.

(b) Huruvida en lösensumma betalades och om så är fallet, vilket belopp, vilket betalningssätt och till vilken mottagare eller mottagande sida, inbegripet leverantören av kryptotillgångar och leverantören av kryptotillgångstjänster, i förekommande fall.”

(9) I artikel 24 ska följande punkter läggas till som punkterna 4, 5 och 6:

”4. För att visa efterlevnad av artikel 21 får medlemsstaterna kräva att väsentliga och viktiga entiteter erhåller ett certifikat om cybersäkerhetsstatus enligt en europeisk ordning för cybersäkerhetscertifiering som antagits i enlighet med artikel 75 i förordning (EU) XXX/XXX * * * * [förslag till CSA2].

5. Om en väsentlig eller viktig entitets cybersäkerhetsstatus är certifierad enligt en europeisk ordning för cybersäkerhetscertifiering som antagits i enlighet med artikel 74 i förordning (EU) XXX/XXX * * * * * [förslag till CSA2] och om certifikatet visar att de krav som fastställs i en genomförandeakt som antagits i enlighet med artikel 21.5 i detta direktiv eller nationell rätt som införlivar artikel 21.1 och 21.2 i detta direktiv efterlevs, får de behöriga myndigheterna inte underställa entiteten ytterligare åtgärder i enlighet med artikel 32.2 b eller artikel 33.2 b, beroende på vad som är tillämpligt med avseende på de krav som omfattas av certifikatet.

6. En certifiering enligt punkt 4 ska inte påverka den väsentliga eller viktiga entitetens ansvar för att efterleva detta direktiv.

_____

* * * * förordning (EU) XXX/XXX [förslag till CSA2].”

(10) Artikel 26 ska ändras på följande sätt:

(a) I punkt 1 ska följande led läggas till som led d:

”d) Lufttrafikföretag, som ska anses omfattas av jurisdiktionen i den medlemsstat vars behöriga tillståndsmyndighet utfärdade den operativa licensen för verksamhetsutövaren i enlighet med Europaparlamentets och rådets förordning (EG) nr 1008/2008 * * * * *, eller, om den operativa licensen eller motsvarande inte har utfärdats i enlighet med den förordningen, som ska anses omfattas av jurisdiktionen i den medlemsstat där de har sitt huvudsakliga etableringsställe i unionen i enlighet med punkt 2.

_____

***** Europaparlamentets och rådets förordning (EG) nr 1008/2008 av den 24 september 2008 om gemensamma regler för tillhandahållande av lufttrafik i gemenskapen (EUT L 293, 31.10.2008, s. 3, ELI: http://data.europa.eu/eli/reg/2008/1008/oj).”

(b) Punkt 3 ska ersättas med följande:

”3. Om en väsentliga eller viktig entitet inte är etablerad i unionen, men erbjuder tjänster inom unionen, ska den utse en företrädare i unionen. Företrädaren ska vara etablerad i en av de medlemsstater där tjänsterna erbjuds. Entiteten ska anses omfattas av jurisdiktionen i den medlemsstat där företrädaren är etablerad. Om en sådan entitet är en entitet som avses i punkt 1 a, ska den anses omfattas av jurisdiktionen i den medlemsstat där den tillhandahåller sina tjänster. Om det inte finns en utsedd företrädare i unionen enligt denna punkt får varje medlemsstat där entiteten tillhandahåller tjänster vidta rättsliga åtgärder mot entiteten för överträdelsen av detta direktiv.”

(11) Artikel 27 ska ändras på följande sätt:

(a) Punkt 1 ska ersättas med följande:

”1. Enisa ska skapa och upprätthålla ett register över väsentliga och viktiga entiteter samt entiteter som tillhandahåller domännamnsregistreringstjänster, på grundval av den information som mottagits från de gemensamma kontaktpunkterna i enlighet med punkt 4. Enisa ska på begäran ge de behöriga myndigheterna tillgång till information om leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, entiteter som tillhandahåller

domännamnsregistreringstjänster, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leveransleverans av innehåll, leverantörer av utlokaliserade driftstjänster, leverantörer av utlokaliserade säkerhetstjänster samt leverantörer av internetbaserade marknadsplatser online, av internetbaserade sökmotorer och av plattformar för sociala nätverkstjänster och lufttrafikföretag som lagras i det registret, samtidigt som skydd av informationens konfidentialitet säkerställs i tillämpliga fall.”

(b) Punkt 2 ska utgå.

(c) Punkterna 3, 4 och 5 ska ersättas med följande:

”3. Medlemsstaterna ska säkerställa att de väsentliga och viktiga entiteterna underrättar den behöriga myndigheten om alla ändringar av de uppgifter som de lämnat enligt artikel 3.4 utan dröjsmål och under alla omständigheter inom två veckor från dagen för ändringen.

4. När den gemensamma kontaktpunkten i den berörda medlemsstaten mottagit den information som avses i artikel 3.4, ska den utan dröjsmål vidarebefordra den informationen till Enisa.

5. Den information som avses i artikel 3.4 första stycket ska, i tillämpliga fall, lämnas genom den nationella mekanism som avses i artikel 3.4 fjärde stycket.”

(12) Följande artikel ska införas som artikel 37a:

”Artikel 37a

Enisas roll i det ömsesidiga biståndet

1. Enisa ska bistå medlemsstaterna vid tillhandahållandet av ömsesidigt bistånd i den mening som avses i artikel 37 och bidra till att underlätta sådana samarbetsprocesser för väsentliga och viktiga entiteter som tillhandahåller tjänster i mer än en medlemsstat eller som tillhandahåller tjänster i en eller flera medlemsstater och vars nätverks- och informationssystem är belägna i en eller flera andra medlemsstater.

2. För tillämpningen av punkt 1 ska Enisa senast den... [15 månader efter denna förordnings ikraftträdande] genomföra en heltäckande analys av gränsöverskridande cybersäkerhetsrisker som rör väsentliga och viktiga entiteter som tillhandahåller tjänster i mer än en medlemsstat eller som tillhandahåller tjänster i en eller flera medlemsstater och vars nätverks- och informationssystem är belägna i en eller flera andra medlemsstater. I analysen ska en utvärdering göras av omfattningen av möjliga gränsöverskridande konsekvenser, och konsekvenser för den inre marknaden, av incidenter som påverkar sådana väsentliga och viktiga entiteter. Vid denna analys ska Enisa, i samarbete med kommissionen och samarbetsgruppen, utarbeta en metod. På grundval av analysen ska Enisa utarbeta en rapport om den övergripande bedömningen av gränsöverskridande cybersäkerhetsrisker, som ska uppdateras årligen.

3. På grundval av rapporten om den övergripande bedömningen av gränsöverskridande cybersäkerhetsrisker ska Enisa

(a) vid behov rekommendera de relevanta behöriga myndigheterna att inrätta gemensamma undersökningsgrupper för att stödja tillsynen av specifika enheter,

(b) utarbeta riktlinjer för gemensamma tillsynsåtgärder,

(c) på begäran av de behöriga myndigheterna i de berörda medlemsstaterna fastställa praktiska arrangemang för genomförandet av gemensamma tillsynsåtgärder,

(d) på begäran av de behöriga myndigheterna i de berörda medlemsstaterna och med förbehåll för och i proportion till sina egna resurser, delta i gemensamma tillsynsåtgärder,

(e) på begäran av de berörda medlemsstaternas behöriga myndigheter bistå vid bedömningen av en väsentlig eller viktig entitets grad av genomförande av de riskhanteringsåtgärder för cybersäkerhet som fastställs i artikel 21.

4. Vid tillämpning av punkt 3 e i denna artikel ska de behöriga myndigheterna i de berörda medlemsstaterna i förekommande fall förse Enisa med en förteckning över de riskhanteringsåtgärder för cybersäkerhet som vidtagits av den väsentliga eller viktiga entiteten i enlighet med artikel 21, en förteckning över de tillsyns- eller efterlevnadskontrollåtgärder som vidtagits samt relevant dokumentation, inbegripet bevis på genomförande av cybersäkerhetspolicyer, såsom resultaten av säkerhetsrevisioner, som de behöriga myndigheterna har gjort i enlighet med artiklarna 32 och 33 med avseende på den entiteten.

5. Om en medlemsstat erhåller ömsesidigt bistånd enligt artikel 37.1 första stycket c, ska den gemensamma kontaktpunkten informera Enisa om att ömsesidigt bistånd ägde rum. I tillämpliga fall ska den gemensamma kontaktpunkten ange vilken gränsöverskridande incident enligt artikel 23.6 som var kopplad till fallet av ömsesidigt bistånd.”

(13) Bilagorna I och II ska ändras i enlighet med bilagan till detta direktiv.

Artikel 2
Införlivande

1. Senast den … [12 månader efter detta direktivs ikraftträdande] ska medlemsstaterna anta och offentliggöra de bestämmelser som är nödvändiga för att följa detta direktiv. De ska genast underrätta kommissionen om detta.

De ska tillämpa dessa bestämmelser från och med den ... [en dag efter den dag som avses i första stycket].

2. När en medlemsstat antar de bestämmelser som avses i punkt 1 ska de innehålla en hänvisning till detta direktiv eller åtföljas av en sådan hänvisning när de offentliggörs. Närmare föreskrifter om hur hänvisningen ska göras ska varje medlemsstat själv utfärda.

Artikel 3
Ikraftträdande

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

Artikel 4

Adressater

Detta direktiv riktar sig till medlemsstaterna.

Utfärdat i Strasbourg den

På Europaparlamentets vägnar	*På rådets vägnar*
Ordförande	*Ordförande*
[...]	*[...]*