EUROPAPARLAMENTS- OG RÅDSDIREKTIV (EU) 2016/1148 2024/EØS/63/36

av 6. juli 2016

om tiltak for å sikre et høyt felles nivå for sikkerhet i nettverks- og informasjonssystemer i hele Unionen(*)

EUROPAPARLAMENTET OG RÅDET FOR DEN EUROPEISKE UNION HAR

under henvisning til traktaten om Den europeiske unions virkemåte, særlig artikkel 114,

under henvisning til forslag fra Europakommisjonen,

etter oversending av utkast til regelverksakt til de nasjonale parlamentene,

under henvisning til uttalelse fra Den europeiske økonomiske og sosiale komité([1]),

etter den ordinære regelverksprosessen([2]) og

ut fra følgende betraktninger:

1) Nettverks- og informasjonssystemer og nettverks- og informasjonstjenester har en viktig rolle i samfunnet. At disse systemene er pålitelige og sikre, er av avgjørende betydning for økonomisk og samfunnsmessig virksomhet, og særlig for det indre markeds funksjon.

2) Omfanget, hyppigheten og virkningen av sikkerhetshendelser er økende og utgjør en alvorlig trussel mot nettverks- og informasjonssystemer. Disse systemene kan også bli mål for forsettlige handlinger som har til hensikt å skade eller forstyrre driften av systemene. Slike hendelser kan være til hinder for økonomisk virksomhet, medføre betydelige økonomiske tap, undergrave brukernes tillit og få store negative konsekvenser for Unionens økonomi.

3) Nettverks- og informasjonssystemer, særlig internett, er avgjørende for at varer, tjenester og personer fritt kan krysse landegrensene. På grunn av dette tverrnasjonale aspektet kan betydelige forstyrrelser i disse systemene, enten de er tilsiktet eller utilsiktet, og uansett hvor de finner sted, påvirke medlemsstatene hver for seg og Unionen som helhet. Sikkerheten i nettverks- og informasjonssystemer er derfor avgjørende for et velfungerende indre marked.

4) På grunnlag av de betydelige framskrittene som er gjort i det europeiske forumet for medlemsstater når det gjelder å fremme drøftinger og utveksling av god praksis, herunder utarbeiding av prinsipper for et europeisk samarbeid i tilfelle cyberkriser, bør det opprettes en samarbeidsgruppe bestående av representanter for medlemsstatene, Kommisjonen og Den europeiske unions byrå for nettverks- og informasjonssikkerhet («ENISA») for å fremme strategisk samarbeid

(*) Denne unionsrettsakten, kunngjort i EUT L 194 av 19.7.2016, s. 1, er omhandlet i EØS-komiteens beslutning nr. 21/2023 av 3. februar 2023 om endring av EØS-avtalens vedlegg XI (Elektronisk kommunikasjon, audiovisuelle tjenester og informasjonssamfunnstjenester) og protokoll 37 om listen omhandlet i artikkel 101, se EØS-tillegget til *Den europeiske unions tidende* nr. 75 av 19.10.2023, s. 32.

([1]) EUT C 271 av 19.9 2013, s. 133.

([2]) Europaparlamentets holdning av 13. mars 2014 (ennå ikke offentliggjort i EUT) og Rådets holdning ved første behandling av 17. mai 2016 (ennå ikke offentliggjort i EUT). Europaparlamentets holdning av 6. juli 2016 (ennå ikke offentliggjort i EUT).

mellom medlemsstatene om sikkerhet i nettverks- og informasjonssystemer. For at gruppen skal være effektiv og inkluderende, er det viktig at alle medlemsstater har et minimum av ressurser og en strategi som sikrer et høyt sikkerhetsnivå i nettverks- og informasjonssystemer på eget territorium. I tillegg bør ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester være underlagt sikkerhets- og meldingskrav med henblikk på å fremme en kultur for risikohåndtering og sikre at de mest alvorlige hendelsene blir rapportert.

5) De eksisterende ressursene er ikke tilstrekkelige til å sikre et høyt sikkerhetsnivå i nettverks- og informasjonssystemene i Unionen. Medlemsstatene har svært ulike beredskapsnivåer, noe som har ført til forskjellige tilnærmingsmåter i Unionen. Dette fører til ulikheter i vernet av forbrukere og foretak og undergraver det samlede sikkerhetsnivået i nettverks- og informasjonssystemer i Unionen. Mangelen på felles krav til ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester gjør det i sin tur umulig å få på plass en overordnet og effektiv ordning for samarbeid på unionsplan. Universiteter og forskningssentre er avgjørende for å stimulere til forskning, utvikling og innovasjon på disse områdene.

6) For å håndtere sikkerhetsutfordringene i nettverks- og informasjonssystemer på en effektiv måte kreves det derfor en helhetlig tilnærming på unionsplan som omfatter felles minstekrav til kapasitetsoppbygging og planlegging, informasjonsutveksling, samarbeid og felles sikkerhetskrav til ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester. Ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester er imidlertid ikke forhindret fra å gjennomføre sikkerhetstiltak som er strengere enn dem som fastsettes i dette direktivet.

7) For å dekke alle relevante hendelser og risikoer bør dette direktivet få anvendelse både på ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester. Forpliktelsene som innføres for ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester, bør imidlertid ikke gjelde for foretak som leverer offentlige kommunikasjonsnett eller offentlig tilgjengelige elektroniske kommunikasjonstjenester som definert i europaparlaments- og rådsdirektiv 2002/21/EF([3]), som omfattes av de særlige sikkerhets- og integritetskravene fastsatt i det direktivet, og heller ikke for ytere av tillitstjenester som definert i europaparlaments- og rådsforordning (EU) nr. 910/2014([4]), som omfattes av sikkerhetskravene fastsatt i den forordningen.

8) Dette direktivet bør ikke være til hinder for at hver enkelt medlemsstat treffer nødvendige tiltak for å sikre vern av sine grunnleggende sikkerhetsinteresser, for å opprettholde offentlig orden og sikkerhet og for å muliggjøre etterforskning, avsløring og rettslig forfølging av straffbare forhold. I samsvar med artikkel 346 i traktaten om Den europeiske unions virkemåte (TEUV) er ingen medlemsstat forpliktet til å gi opplysninger dersom den finner at det vil være i strid med dens grunnleggende sikkerhetsinteresser. Rådsbeslutning 2013/488/EU([5]) og fortrolighetsavtaler eller uformelle fortrolighetsavtaler, som «Traffic Light Protocol», er av betydning i denne sammenhengen.

9) Visse økonomiske sektorer er allerede eller kan i framtiden bli regulert av sektorspesifikke unionsrettsakter som inneholder regler om sikkerhet i nettverks- og informasjonssystemer. Når disse unionsrettsaktene inneholder bestemmelser som fastsetter krav vedrørende sikkerhet i nettverks- og informasjonssystemer eller melding av hendelser, bør disse bestemmelsene få anvendelse dersom de inneholder krav som har minst tilsvarende virkning som forpliktelsene i dette direktivet. Medlemsstatene bør da anvende bestemmelsene i slike sektorspesifikke unionsrettsakter, herunder bestemmelsene om jurisdiksjon, og bør ikke gjennomføre identifikasjonsprosessen for ytere av samfunnsviktige tjenester som definert i dette direktivet. I den forbindelse bør medlemsstatene gi Kommisjonen opplysninger om anvendelsen av slike *lex specialis*-bestemmelser. Når det skal avgjøres om de kravene til sikkerhet i nettverks- og informasjonssystemer og melding av hendelser som er fastsatt i sektorspesifikke unionsrettsakter, tilsvarer kravene i dette direktivet, bør det bare tas hensyn til bestemmelsene i relevante unionsrettsakter og til deres anvendelse i medlemsstatene.

10) I sjøfartssektoren omfatter de sikkerhetskravene som stilles til rederier, fartøyer, havneanlegg, havner og sjøtrafikksentraler i henhold til unionsrettsakter, alle deler av virksomheten, også radio- og telekommunikasjonsutstyr, datasystemer og nettverk. De obligatoriske prosedyrene som skal følges, omfatter blant annet rapportering av alle hendelser, og bør derfor anses som *lex specialis*, forutsatt at disse kravene minst er likeverdige med de tilsvarende bestemmelsene i dette direktivet.

([3]) Europaparlaments- og rådsdirektiv 2002/21/EF av 7. mars 2002 om felles rammeregler for elektroniske kommunikasjonsnett og -tjenester (rammedirektivet) (EFT L 108 av 24.4.2002, s. 33).

([4]) Europaparlaments- og rådsforordning (EU) nr. 910/2014 av 23. juli 2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked og om oppheving av direktiv 1999/93/EF (EUT L 257 av 28.8.2014, s. 73).

([5]) Rådsbeslutning 2013/488/EU av 23. september 2013 om sikkerhetsregler for vern av graderte EU-opplysninger (EUT L 274 av 15.10.2013, s. 1).

11) Når medlemsstatene identifiserer operatører i sjøfartssektoren, bør de ta hensyn til eksisterende og kommende internasjonale regler og retningslinjer, særlig de som utarbeides av Den internasjonale sjøfartsorganisasjon, med sikte på å tilby de enkelte sjøfartsoperatørene en enhetlig tilnærming.

12) Reguleringen av og tilsynet med banksektoren og sektoren for finansmarkedsinfrastrukturer er i høy grad harmonisert på unionsplan ved hjelp av primær og sekundær EU-rett samt standarder utviklet i samarbeid med de europeiske tilsynsmyndighetene. Innenfor bankunionen sikres anvendelsen av og tilsynet med disse kravene gjennom den felles tilsynsordningen. For medlemsstater som ikke er en del av bankunionen, sikres dette av medlemsstatenes banktilsynsmyndigheter. På andre områder av finanssektorreguleringen bidrar også Det europeiske finanstilsynssystem til å sikre høy grad av likhet og tilnærming i tilsynspraksis. Den europeiske verdipapir- og markedstilsynsmyndighet fører også direkte tilsyn med visse enheter, nærmere bestemt kredittvurderingsbyråer og transaksjonsregistre.

13) Operasjonell risiko er en viktig del av reguleringen av og tilsynet med banksektoren og sektoren for finansmarkedsinfrastrukturer. Den omfatter alle deler av virksomheten, også nettverks- og informasjonssystemers sikkerhet, funksjonsdyktighet og robusthet. Kravene til disse systemene, som ofte går lenger enn kravene fastsatt i dette direktivet, er fastsatt i en rekke unionsrettsakter, herunder regler om adgang til å utøve virksomhet som kredittinstitusjon og tilsyn med kredittinstitusjoner og verdipapirforetak samt regler om tilsynskrav for kredittinstitusjoner og verdipapirforetak, som omfatter krav vedrørende operasjonell risiko, regler om markeder for finansielle instrumenter, som omfatter krav vedrørende risikovurdering for verdipapirforetak og for regulerte markeder, regler om OTC-derivater, sentrale motparter og transaksjonsregistre, som omfatter krav vedrørende operasjonell risiko for sentrale motparter og transaksjonsregistre, og regler om forbedring av oppgjørssystemet for verdipapirer i Unionen og om verdipapirsentraler, som omfatter krav vedrørende operasjonell risiko. Dessuten er krav om melding av hendelser en del av vanlig tilsynspraksis i finanssektoren og finnes ofte i tilsynshåndbøker. Medlemsstatene bør vurdere disse reglene og kravene i sin søknad om *lex specialis*.

14) Som Den europeiske sentralbank bemerket i sin uttalelse av 25. juli 2014([6]), berører dette direktivet ikke den ordningen for Eurosystemets tilsyn med betalings- og oppgjørssystemer som er fastsatt i EU-retten. Det vil være hensiktsmessig for de myndighetene som har ansvar for slikt tilsyn. å utveksle erfaringer om spørsmål som gjelder sikkerhet i nettverks- og informasjonssystemer, med de myndighetene som er vedkommende myndigheter i henhold til dette direktivet. Det samme gjelder for medlemmer av Det europeiske system av sentralbanker som ikke er med i euroområdet, og som fører slikt tilsyn med betalings- og oppgjørssystemer i samsvar med nasjonale lover og forskrifter.

15) En nettbasert markedsplass gjør det mulig for forbrukere og næringsdrivende å inngå nettbaserte salgs- eller tjenesteavtaler med næringsdrivende og er det endelige bestemmelsesstedet for inngåelse av slike avtaler. Den bør ikke omfatte nettbaserte tjenester som bare tjener til å formidle tredjepartstjenester som gir mulighet til å inngå en avtale i siste instans. Den bør derfor ikke omfatte nettbaserte tjenester som sammenligner prisene på bestemte produkter eller tjenester fra forskjellige næringsdrivende og deretter omdirigerer brukeren til den foretrukne næringsdrivende for å kjøpe produktet. Datatjenester som leveres av den nettbaserte markedsplassen, kan omfatte behandling av transaksjoner, aggregering av data eller profilering av brukere. Applikasjonsbutikker, som fungerer som nettbutikker der applikasjoner eller programvare fra tredjeparter kan distribueres digitalt, skal anses som en type nettbasert markedsplass.

16) En nettbasert søkemotor gjør det mulig for brukeren å foreta søk på i prinsippet alle nettsteder etter innhold om et hvilket som helst emne. Den kan også være rettet mot nettsteder på et bestemt språk. Definisjonen av en nettbasert søkemotor i dette direktivet bør ikke omfatte søkefunksjoner som er begrenset til innholdet på et bestemt nettsted, uansett om søkefunksjonen drives av en ekstern søkemotor. Den bør heller ikke omfatte nettbaserte tjenester som sammenligner priser på bestemte produkter eller tjenester fra forskjellige næringsdrivende og deretter omdirigerer brukeren til den foretrukne næringsdrivende for å kjøpe produktet.

17) Skytjenester omfatter et bredt spekter av aktiviteter som kan leveres i henhold til ulike modeller. Ved anvendelsen av dette direktivet dekker begrepet «skytjenester» tjenester som gir tilgang til en skalerbar og elastisk samling av delbare databehandlingsressurser. Disse databehandlingsressursene omfatter ressurser som nettverk, servere eller annen infrastruktur, lagring, applikasjoner og tjenester. Med begrepet «skalerbar» menes databehandlingsressurser som tilbyderen av skytjenester fordeler på en fleksibel måte, uavhengig av ressursenes geografiske plassering, for å håndtere svingninger i etterspørselen. Begrepet «elastisk samling» brukes til å beskrive databehandlingsressurser som stilles til

([6]) EUT C 352 av 7.10.2014, s. 4.

rådighet og frigjøres på grunnlag av etterspørsel, slik at de tilgjengelige ressursene raskt kan økes eller minskes i takt med arbeidsmengden. Begrepet «delbar» brukes til å beskrive databehandlingsressurser som leveres til flere brukere som har felles tilgang til tjenesten, men der databehandlingen utføres separat for hver enkelt bruker, selv om tjenesten leveres fra samme elektroniske utstyr.

18) Funksjonen til et samtrafikkpunkt på internett (IXP) er å kople sammen nettverk. En IXP gir ikke nettverkstilgang og fungerer ikke som transittleverandør eller transittoperatør. En IXP utfører heller ikke andre tjenester som ikke er knyttet til samtrafikk, men dette hindrer ikke en IXP-operatør i å yte slike andre tjenester. Formålet med en IXP er å kople sammen nettverk som er teknisk og organisatorisk atskilt. Begrepet «autonomt system» brukes til å beskrive et teknisk frittstående nettverk.

19) Medlemsstatene bør ha ansvar for å avgjøre hvilke enheter som oppfyller kriteriene i definisjonen av en yter av samfunnsviktige tjenester. For å sikre en ensartet tilnærming bør definisjonen av en yter av samfunnsviktige tjenester anvendes konsekvent i alle medlemsstater. For dette formålet inneholder dette direktivet bestemmelser om vurdering av enheter som er aktive i bestemte sektorer og delsektorer, om utarbeiding av en liste over samfunnsviktige tjenester, om å ta i betraktning en felles liste over tverrsektorielle faktorer for å avgjøre om en potensiell hendelse kan ha en betydelig forstyrrende innvirkning, om en samrådsprosess mellom relevante medlemsstater når det gjelder enheter som leverer tjenester i mer enn én medlemsstat, og om støtte til samarbeidsgruppen i identifikasjonsprosessen. For å sikre at eventuelle endringer i markedet gjenspeiles på riktig måte, bør listen over identifiserte tjenesteytere regelmessig revideres av medlemsstatene og ajourføres ved behov. Endelig bør medlemsstatene gi Kommisjonen de opplysningene som er nødvendige for å vurdere i hvilken grad denne felles metoden har gjort det mulig for medlemsstatene å anvende definisjonen konsekvent.

20) Når medlemsstatene skal identifisere ytere av samfunnsviktige tjenester, bør de, minst for hver delsektor som er omhandlet i dette direktivet, vurdere hvilke tjenester som må anses som avgjørende for å opprettholde kritisk samfunnsmessig og økonomisk virksomhet, og om de enhetene som er oppført på listen over sektorer og delsektorer omhandlet i dette direktivet, og som leverer disse tjenestene, oppfyller kriteriene for identifikasjon av tjenesteytere. Ved vurderingen av om en enhet yter en tjeneste som er avgjørende for å opprettholde kritisk samfunnsmessig eller økonomisk virksomhet, er det tilstrekkelig å undersøke om enheten yter en tjeneste som er oppført på listen over samfunnsviktige tjenester. Videre bør det dokumenteres at det kreves nettverks- og informasjonssystemer for å yte den samfunnsviktige tjenesten. Endelig bør medlemsstatene når de vurderer om en hendelse kan ha en betydelig forstyrrende innvirkning på leveringen av tjenesten, ta hensyn til en rekke tverrsektorielle og, når det er relevant, sektorspesifikke faktorer.

21) Ved identifikasjon av ytere av samfunnsviktige tjenester menes med virksomhet i en medlemsstat at det effektivt og faktisk utøves av aktivitet gjennom en stabil struktur. En slik strukturs juridiske form, enten det dreier seg om en filial eller et datterforetak med status som juridisk person, er ikke den avgjørende faktoren i den forbindelse.

22) Det er mulig at enheter som opererer i sektorene og delsektorene omhandlet i dette direktivet, yter både samfunnsviktige og ikke-samfunnsviktige tjenester. I luftfartssektoren yter for eksempel lufthavner tjenester som en medlemsstat kan anse som samfunnsviktige, så som forvaltning av rullebanene, men også en rekke tjenester som kan anses som ikke-samfunnsviktige, så som å stille butikklokaler til rådighet. Ytere av samfunnsviktige tjenester bør være underlagt de særlige sikkerhetskravene bare med hensyn til de tjenestene som anses som samfunnsviktige. Med henblikk på identifikasjon av tjenesteytere bør medlemsstatene derfor utarbeide en liste over tjenester som anses som samfunns-viktige.

23) Listen bør inneholde alle tjenester som ytes på territoriet til en gitt medlemsstat, og som oppfyller kravene i dette direktivet. Medlemsstatene bør ha mulighet til å supplere den eksisterende listen ved å tilføye nye tjenester. Listen over tjenester bør fungere som et referansepunkt for medlemsstatene og gjøre det mulig å identifisere ytere av samfunnsviktige tjenester. Formålet med listen er å identifisere de typene av samfunnsviktige tjenester i en bestemt sektor som omhandles i dette direktivet, slik at de kan holdes atskilt fra ikke-samfunnsviktige tjenester som en enhet som er aktiv i en bestemt sektor, kan være ansvarlig for. Den listen over tjenester som hver enkelt medlemsstat utarbeider, vil kunne bidra ytterligere til vurderingen av hver medlemsstats lovgivningsmessige praksis, slik at det kan sikres en overordnet konsekvens i identifikasjonsprosessen mellom medlemsstatene.

24) Når en enhet yter en samfunnsviktig tjeneste i to eller flere medlemsstater, bør disse medlemsstatene ha bilaterale eller multilaterale drøftinger i forbindelse med identifikasjonsprosessen. Denne samrådsprosessen er ment å hjelpe dem med å vurdere om den aktuelle tjenesteyteren er av kritisk betydning når det gjelder virkninger på tvers av landegrensene, hvilket gir hver berørt medlemsstat mulighet til å framlegge sine synspunkter på risikoene forbundet med de tjenestene som ytes. I denne prosessen bør de berørte medlemsstatene ta hensyn til hverandres synspunkter, og de bør i den forbindelse kunne be om bistand fra samarbeidsgruppen.

25) Etter identifikasjonsprosessen bør medlemsstatene vedta nasjonale tiltak for å avgjøre hvilke enheter som er underlagt forpliktelser med hensyn til sikkerheten i nettverks- og informasjonssystemer. Dette kan oppnås ved å vedta en liste over alle ytere av samfunnsviktige tjenester eller ved å vedta nasjonale tiltak som bygger på objektive, målbare kriterier, for eksempel tjenesteyterens produksjon eller antallet brukere, som gjør det mulig å avgjøre hvilke enheter som er underlagt forpliktelser med hensyn til sikkerheten i nettverks- og informasjonssystemer. De nasjonale tiltakene, uansett om de allerede er vedtatt eller om de vedtas innenfor rammen av dette direktivet, bør omfatte alle rettslige tiltak, administrative tiltak og strategier som gjør det mulig å identifisere ytere av samfunnsviktige tjenester i henhold til dette direktivet.

26) For å gi en indikasjon på hvilken betydning identifiserte ytere av samfunnsviktige tjenester har i den aktuelle sektoren, bør medlemsstatene ta hensyn til antallet av og størrelsen på disse tjenesteyterne, for eksempel målt i markedsandeler eller produsert eller levert mengde, uten å være forpliktet til å røpe opplysninger som vil avsløre hvilke ytere som er identifisert.

27) Når medlemsstatene skal avgjøre om en hendelse kan ha en betydelig forstyrrende innvirkning på en samfunnsviktig tjeneste, bør de ta hensyn til en rekke ulike faktorer, for eksempel antall brukere som er avhengige av tjenesten til private eller yrkesmessige formål. Bruken av tjenesten kan skje direkte, indirekte eller gjennom formidling. Når medlemsstatene skal vurdere hvilken innvirkning en hendelse kan ha, i form av omfang og varighet, på økonomisk og samfunnsmessig virksomhet eller offentlig sikkerhet, bør de også vurdere hvor lang tid det er sannsynlig at det vil ta før avbruddet får en negativ innvirkning.

28) I tillegg til tverrsektorielle faktorer bør de også vurdere sektorspesifikke faktorer for å avgjøre om en hendelse kan ha en betydelig forstyrrende innvirkning på leveringen av en samfunnsviktig tjeneste. For energileverandører kan slike faktorer for eksempel være mengden eller andelen av den nasjonalt produserte energien; for oljeleverandører mengden olje per dag; for lufttransport, herunder lufthavner og luftfartsselskaper, samt for jernbanetransport og sjøhavner, andelen av den nasjonale trafikkmengden og antallet passasjerer eller fraktoperasjoner per år; for bankvirksomhet eller finansmarkedsinfrastrukturer deres systemiske betydning basert på totale eiendeler eller forholdet mellom disse eiendelene og BNP; for helsesektoren antallet pasienter under tjenesteyterens behandling per år; for vannproduksjon, -behandling og -forsyning vannmengden samt antallet og typene av brukere som forsynes, herunder for eksempel sykehus, organisasjoner i offentlig sektor eller enkeltpersoner, og om det finnes alternative vannkilder som dekker samme geografiske område.

29) For å oppnå og opprettholde et slikt høyt sikkerhetsnivå bør hver medlemsstat ha en nasjonal strategi for sikkerhet i nettverks- og informasjonssystemer som definerer de strategiske målene og de konkrete politiske tiltakene som skal gjennomføres.

30) På bakgrunn av forskjellene i nasjonale styringsstrukturer, for å sikre eksisterende sektorspesifikke ordninger eller Unionens tilsyns- og reguleringsorganer og for å unngå dobbeltarbeid bør medlemsstatene kunne utpeke mer enn én vedkommende nasjonal myndighet med ansvar for å utføre oppgavene knyttet til sikkerhet i nettverks- og informasjonssystemene til ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester i henhold til dette direktivet.

31) For å fremme samarbeid og kommunikasjon over landegrensene og gjøre det mulig å gjennomføre dette direktivet effektivt må hver medlemsstat, uten at det berører sektorspesifikke reguleringsordninger, utpeke et nasjonalt felles kontaktpunkt med ansvar for å samordne spørsmål knyttet til sikkerhet i nettverks- og informasjonssystemer og grensekryssende samarbeid på unionsplan. Vedkommende myndigheter og de felles kontaktpunktene bør ha tilstrekkelige tekniske, økonomiske og menneskelige ressurser til å sikre at de kan utføre sine oppgaver på en effektiv og formålstjenlig måte, og dermed nå målene for dette direktivet. Ettersom dette direktivet har som mål å forbedre det indre markeds funksjon ved å skape tillit og trygghet, må medlemsstatenes organer kunne samarbeide effektivt med økonomiske aktører og ha en struktur som er forenlig med dette.

32) Vedkommende myndigheter eller enhetene for håndtering av digitale hendelser («CSIRT-enheter») bør motta meldinger om hendelser. De felles kontaktpunktene bør ikke motta noen meldinger om hendelser direkte med mindre de også fungerer som en vedkommende myndighet eller en CSIRT-enhet. En vedkommende myndighet eller en CSIRT-enhet bør imidlertid kunne gi det felles kontaktpunktet i oppgave å videreformidle hendelsesmeldinger til de felles kontaktpunktene i andre berørte medlemsstater.

33) For å sikre at medlemsstatene og Kommisjonen får opplysninger på en effektiv måte, bør det felles kontaktpunktet sende en sammenfattende rapport til samarbeidsgruppen, og rapporten bør anonymiseres for å sikre fortrolig behandling av meldingene og av identiteten til ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester, ettersom det ikke er nødvendig å ha opplysninger om melderens identitet for å utveksle beste praksis i samarbeidsgruppen. Den sammenfattende rapporten bør inneholde opplysninger om antall mottatte meldinger og arten av de meldte hendelsene, for eksempel typene av sikkerhetsbrudd og deres alvorlighetsgrad eller varighet.

34) Medlemsstatene bør ha tilstrekkelige tekniske og organisatoriske ressurser til å forebygge, avdekke og håndtere hendelser og risikoer knyttet til nettverks- og informasjonssystemer og til å begrense virkningene av dem. Medlemsstatene bør derfor sikre at de har velfungerende CSIRT-enheter, også kjent som CERT-enheter, som oppfyller grunnleggende krav og kan sikre effektive og kompatible ressurser til å håndtere hendelser og risikoer og sikre effektivt samarbeid på unionsplan. For at alle typer ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester skal kunne dra nytte av slike ressurser og slikt samarbeid, bør medlemsstatene sikre at alle typer omfattes av en utpekt CSIRT-enhet. Med tanke på viktigheten av internasjonalt samarbeid om cybersikkerhet bør CSIRT-enheter kunne delta i internasjonale samarbeidsnettverk i tillegg til det CSIRT-nettverket som opprettes ved dette direktivet.

35) Ettersom de fleste nettverks- og informasjonssystemer drives privat, er samarbeid mellom offentlig og privat sektor avgjørende. Ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester bør oppmuntres til å opprette egne uformelle samarbeidsordninger for å ivareta sikkerheten i nettverks- og informasjonssystemer. Samarbeidsgruppen bør kunne innby berørte parter til drøftingene ved behov. For effektivt å oppmuntre til å utveksle opplysninger og beste praksis er det svært viktig å sikre at ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester som deltar i slik utveksling, ikke påføres noen ulemper som følge av sin deltakelse.

36) ENISA bør bistå medlemsstatene og Kommisjonen ved å bidra med sakkunnskap og rådgivning samt ved å fremme utveksling av beste praksis. Særlig bør Kommisjonen, og bør medlemsstatene kunne, rådføre seg med ENISA ved anvendelsen av dette direktivet. For å bygge opp kapasitet og kunnskap blant medlemsstatene bør samarbeidsgruppen også være et hjelpemiddel til utveksling av beste praksis og drøftinger av medlemsstatenes ressurser og beredskap, og den bør på frivillig grunnlag bistå medlemmene med evaluering av nasjonale strategier for sikkerhet i nettverks- og informasjonssystemer, oppbygging av kapasitet og evaluering av øvelser knyttet til sikkerheten i nettverks- og informasjonssystemer.

37) Når det er hensiktsmessig, bør medlemsstatene kunne benytte eller tilpasse eksisterende organisasjonsstrukturer eller strategier når de anvender dette direktivet.

38) De respektive oppgavene til samarbeidsgruppen og ENISA er avhengige av hverandre og utfyller hverandre. Generelt bør ENISA bistå samarbeidsgruppen med utførelsen av dens oppgaver i samsvar med ENISAs mål i henhold til europaparlaments- og rådsforordning (EU) nr. 526/2013([7]), som er å bistå Unionens institusjoner, organer, kontorer og byråer og medlemsstatene med å gjennomføre den politikken som er nødvendig for å oppfylle de lovfestede og forskriftsmessige kravene til sikkerhet i nettverks- og informasjonssystemer i henhold til gjeldende og framtidige unionsrettsakter. ENISA bør særlig yte bistand på de områdene som svarer til ENISAs egne oppgaver som fastsatt i forordning (EU) nr. 526/2013, som er å analysere strategier for sikkerhet i nettverks- og informasjonssystemer, støtte organisering og gjennomføring av øvelser på unionsplan som gjelder sikkerhet i nettverks- og informasjonssystemer, samt utveksle opplysninger om og beste praksis for bevisstgjøring og opplæring. ENISA bør også delta i utarbeidingen av retningslinjer for sektorspesifikke kriterier som skal brukes for å fastslå hvor stor innvirkning en hendelse har.

([7]) Europaparlaments- og rådsforordning (EU) nr. 526/2013 av 21. mai 2013 om Den europeiske unions byrå for nettverks- og informasjonssikkerhet (ENISA) og om oppheving av forordning (EF) nr. 460/2004 (EUT L 165 av 18.6.2013, s. 41).

39) For å fremme forbedret sikkerhet i nettverks- og informasjonssystemer bør samarbeidsgruppen ved behov samarbeide med Unionens relevante institusjoner, organer, kontorer og byråer for å utveksle kunnskap og beste praksis samt gi råd om sikkerhetsaspekter ved nettverks- og informasjonssystemer som kan påvirke deres arbeid, samtidig som gjeldende ordninger for utveksling av fortrolige opplysninger respekteres. I samarbeidet med rettshåndhevende myndigheter om sikkerhetsaspekter ved nettverkverks- og informasjonssystemer som kan påvirke disse myndighetenes arbeid, bør samarbeidsgruppen respektere eksisterende informasjonskanaler og etablerte nettverk.

40) Opplysninger om hendelser blir stadig mer verdifulle for allmennheten og for foretak, særlig små og mellomstore bedrifter. I noen tilfeller er slike opplysninger allerede tilgjengelige via nettsteder på nasjonalt plan, på et bestemt lands språk, og først og fremst om hendelser og tilfeller med en nasjonal dimensjon. Ettersom foretak i økende grad opererer på tvers av landegrensene og borgerne bruker nettbaserte tjenester, bør opplysninger om hendelser gis i aggregert form på unionsplan. CSIRT-nettverkets sekretariat oppfordres til å opprette et nettsted eller en særskilt side på et eksisterende nettsted der generelle opplysninger om større hendelser som har funnet sted i Unionen, gjøres tilgjengelige for allmennheten, med særlig fokus på interessene og behovene til foretak. CSIRT-enheter som deltar i CSIRT-nettverket, oppfordres til frivillig å overlevere de opplysningene som skal offentliggjøres på nettstedet, uten å inkludere fortrolige eller følsomme opplysninger.

41) Dersom opplysninger anses som fortrolige i samsvar med Unionens og nasjonale regler for forretningshemmeligheter, bør denne fortroligheten ivaretas ved utførelsen av oppgavene og oppfyllelsen av målene i dette direktivet.

42) Øvelser som simulerer hendelsesscenarioer i sanntid, er avgjørende for å teste medlemsstatenes beredskap og samarbeid når det gjelder sikkerhet i nettverks- og informasjonssystemer. Øvelsesserien CyberEurope, som ENISA samordner med deltakelse fra medlemsstatene, er et nyttig verktøy for å teste og utarbeide anbefalinger om hvordan håndteringen av hendelser på unionsplan bør forbedres over tid. Ettersom medlemsstatene for øyeblikket verken er forpliktet til å planlegge eller å delta i øvelser, bør opprettelsen av CSIRT-nettverket i henhold til dette direktivet gi medlemsstatene mulighet til å delta i øvelser på grunnlag av nøyaktig planlegging og strategiske valg. Samarbeidsgruppen som opprettes i henhold til dette direktivet, bør drøfte de strategiske beslutningene om øvelser, særlig, men ikke utelukkende, når det gjelder hyppigheten av øvelsene og utformingen av scenarioene. ENISA bør i samsvar med sitt mandat støtte organiseringen og gjennomføringen av øvelser på unionsplan ved å bistå samarbeidsgruppen og CSIRT-nettverket med sakkunnskap og råd.

43) Tatt i betraktning at sikkerhetsproblemer som påvirker nettverks- og informasjonssystemer, har en global dimensjon, er det behov for tettere internasjonalt samarbeid for å forbedre sikkerhetsstandardene og informasjonsutvekslingen og for å fremme en felles, helhetlig tilnærming til sikkerhetsspørsmål.

44) Ansvaret for å ivareta sikkerheten i nettverks- og informasjonssystemer ligger for en stor del hos ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester. En kultur for risikohåndtering, som omfatter risikovurdering og gjennomføring av sikkerhetstiltak som står i forhold til risikoene, bør fremmes og utvikles gjennom passende lovgivningsmessige krav og frivillige bransjeordninger. Å skape pålitelige og like vilkår er også avgjørende for at samarbeidsgruppen og CSIRT-nettverket skal være velfungerende, slik at det sikres effektivt samarbeid fra alle medlemsstater.

45) Dette direktivet får anvendelse bare på offentlige forvaltninger som er identifisert som ytere av samfunnsviktige tjenester. Det er derfor medlemsstatenes ansvar å ivareta sikkerheten i nettverks- og informasjonssystemer tilhørende offentlige forvaltninger som ikke faller inn under dette direktivets virkeområde.

46) Risikohåndteringstiltak omfatter tiltak for å identifisere alle risikoer for hendelser, med det formålet å forebygge, avdekke og håndtere hendelser og begrense virkningene av dem. Sikkerhet i nettverks- og informasjonssystemer omfatter sikkerhet for data som lagres, overføres og behandles.

47) Vedkommende myndigheter bør beholde retten til å vedta nasjonale retningslinjer om hvilke omstendigheter som forplikter ytere av samfunnsviktige tjenester til å melde fra om hendelser.

48) Mange foretak i Unionen er avhengige av tilbydere av digitale tjenester for å kunne levere tjenestene sine. Ettersom visse digitale tjenester kan være en viktig ressurs for brukerne av dem, også for ytere av samfunnsviktige tjenester, og ettersom disse brukerne ikke alltid har tilgjengelige alternativer, bør dette direktivet også gjelde for tilbydere av digitale tjenester. For mange foretak er sikkerhet, kontinuitet og pålitelighet i den typen digitale tjenester som er omhandlet i dette direktivet, avgjørende for at de skal fungere godt. Et avbrudd i en slik digital tjeneste vil kunne hindre levering av andre tjenester som er avhengige av den, og dermed påvirke viktig økonomisk og samfunnsmessig virksomhet i Unionen. Slike digitale tjenester kan derfor være av vesentlig betydning for en velfungerende drift av foretak som er avhengige av dem, og for at disse foretakene skal kunne delta i det indre marked og i den grensekryssende handelen i Unionen. De tilbyderne av digitale tjenester som omfattes av dette direktivet, er slike som anses å tilby digitale tjenester som mange foretak i Unionen blir stadig mer avhengige av.

49) Tilbydere av digitale tjenester bør sørge for et sikkerhetsnivå som står i forhold til den risikoen de digitale tjenestene deres er utsatt for, tatt i betraktning tjenestenes betydning for virksomheten til andre foretak i Unionen. I praksis er risikoen for ytere av samfunnsviktige tjenester, som ofte er avgjørende for å opprettholde kritisk samfunnsmessig og økonomisk virksomhet, høyere enn for tilbydere av digitale tjenester. Sikkerhetskravene til tilbydere av digitale tjenester bør derfor være mindre strenge. Tilbydere av digitale tjenester bør stå fritt til å treffe tiltak de mener er passende for å håndtere de sikkerhetsrisikoene som nettverks- og informasjonssystemene deres er utsatt for. På grunn av sin tverrnasjonale karakter bør tilbydere av digitale tjenester være gjenstand for en mer harmonisert tilnærming på unionsplan. Gjennomføringsrettsakter bør lette fastsettelsen og gjennomføringen av slike tiltak.

50) Selv om maskinvareprodusenter og programvareutviklere verken er ytere av samfunnsviktige tjenester eller tilbydere av digitale tjenester, øker produktene deres sikkerheten i nettverks- og informasjonssystemer. De spiller derfor en viktig rolle i å gjøre ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester i stand til å sikre nettverks- og informasjonssystemene sine. Slike maskinvare- og programvareprodukter omfattes allerede av regler om produktansvar.

51) Tekniske og organisatoriske tiltak som pålegges ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester, bør ikke forutsette at et bestemt kommersielt produkt innen informasjons- og kommunikasjonsteknologi utformes, utvikles eller produseres på en bestemt måte.

52) Ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester bør ivareta sikkerheten i de nettverks- og informasjonssystemene de bruker. Dette er hovedsakelig private nettverks- og informasjonssystemer som forvaltes av deres interne IT-personale, eller der sikkerhetsoppgavene er utkontraktert. Sikkerhets- og meldingskravene bør gjelde for de relevante yterne av samfunnsviktige tjenester og tilbyderne av digitale tjenester uansett om de vedlikeholder nettverks- og informasjonssystemene sine selv eller utkontrakterer denne oppgaven.

53) For å unngå å pålegge ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester en uforholdsmessig stor økonomisk og administrativ byrde bør kravene stå i forhold til den risikoen som er forbundet med det aktuelle nettverks- og informasjonssystemet, idet det tas hensyn til det aktuelle tekniske utviklingstrinnet for slike tiltak. Med hensyn til tilbydere av digitale tjenester bør disse kravene ikke gjelde for svært små og små bedrifter.

54) Når offentlige forvaltninger i medlemsstatene bruker tjenester fra tilbydere av digitale tjenester, særlig skytjenester, ønsker de kanskje å kunne kreve mer omfattende sikkerhetstiltak fra tilbyderne av disse tjenestene enn det tilbyderne normalt ville tilby for å overholde kravene i dette direktivet. De bør kunne gjøre dette ved hjelp av avtaleforpliktelser.

55) Definisjonene av nettbaserte markedsplasser, nettbaserte søkemotorer og skytjenester i dette direktivet er spesifikke for dette direktivet og berører ikke andre instrumenter.

56) Dette direktivet bør ikke hindre medlemsstatene i å vedta nasjonale tiltak som krever at offentlige organer fastsetter særskilte sikkerhetskrav når de inngår avtaler om skytjenester. Alle slike nasjonale tiltak bør gjelde for det aktuelle offentlige organet og ikke for tilbyderen av skytjenestene.

57) Tatt i betraktning de grunnleggende forskjellene mellom ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester, særlig førstnevntes direkte tilknytning til fysisk infrastruktur og sistnevntes grensekryssende karakter, bør graden av harmonisering for disse to gruppene av enheter differensieres i dette direktivet. For ytere av samfunnsviktige tjenester bør medlemsstatene kunne identifisere de relevante aktørene og innføre strengere krav enn dem som er fastsatt i dette direktivet. Medlemsstatene bør ikke identifisere tilbydere av digitale tjenester, ettersom dette direktivet bør gjelde for alle tilbydere av digitale tjenester innenfor dets virkeområde. I tillegg bør dette direktivet og gjennomførings-rettsaktene som vedtas i henhold til det, sikre høy grad av harmonisering for tilbydere av digitale tjenester med hensyn til sikkerhets- og meldingskrav. Dette bør gjøre det mulig for tilbydere av digitale tjenester å bli behandlet likt over hele Unionen, på en måte som står i forhold til deres karakter og graden av risiko de kan bli utsatt for.

58) Dette direktivet bør ikke være til hinder for at medlemsstatene stiller sikkerhets- og meldingskrav til enheter som ikke er tilbydere av digitale tjenester innenfor direktivets virkeområde, uten at dette berører medlemsstatenes forpliktelser i henhold til unionsretten.

59) Vedkommende myndigheter bør sørge for å bevare uformelle og pålitelige kanaler for informasjonsutveksling. Ved offentliggjøring av hendelser som rapporteres til vedkommende myndigheter, bør allmennhetens interesse av å bli informert om trusler veies behørig opp mot mulige negative konsekvenser for omdømmet og økonomien til de yterne av samfunnsviktige tjenester og tilbyderne av digitale tjenester som rapporterer hendelser. Ved gjennomføringen av meldingsplikten bør vedkommende myndigheter og CSIRT-enhetene ta særlig hensyn til behovet for å holde opplysninger om produktsårbarheter strengt fortrolige fram til det sendes ut egnede sikkerhetsoppdateringer.

60) Tilbydere av digitale tjenester bør være underlagt et mindre strengt, reaktivt tilsyn i ettertid som er tilpasset arten av deres tjenester og virksomhet. Den berørte vedkommende myndigheten bør derfor bare treffe tiltak når den har mottatt dokumentasjon, for eksempel fra tilbyderen av digitale tjenester selv, fra en annen vedkommende myndighet, som kan være vedkommende myndighet i en annen medlemsstat, eller fra en bruker av tjenesten, på at en tilbyder av digitale tjenester ikke oppfyller kravene i dette direktivet, særlig etter at det har inntruffet en hendelse. Vedkommende myndighet bør derfor ikke ha en generell plikt til å føre tilsyn med tilbydere av digitale tjenester.

61) Vedkommende myndigheter bør ha de nødvendige midlene til å utføre sine oppgaver, herunder myndighet til å innhente tilstrekkelige opplysninger til å kunne vurdere sikkerhetsnivået i nettverks- og informasjonssystemer.

62) Hendelser kan være et resultat av kriminell virksomhet som bedre kan forebygges, etterforskes og rettsforfølges gjennom samordning og samarbeid mellom ytere av samfunnsviktige tjenester, tilbydere av digitale tjenester, vedkommende myndigheter og rettshåndhevende myndigheter. Dersom det er mistanke om at en hendelse er knyttet til alvorlig kriminell virksomhet i henhold til unionsretten eller nasjonal rett, bør medlemsstatene oppfordre ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester til å rapportere hendelser av antatt alvorlig strafferettslig art til de relevante rettshåndhevende myndighetene. I relevante tilfeller er det ønskelig at det europeiske senteret for bekjempelse av cyberkriminalitet (EC3) og ENISA legger til rette for samordning mellom forskjellige medlemsstaters vedkommende myndigheter og rettshåndhevende myndigheter.

63) Personopplysninger blir i mange tilfeller satt i fare som følge av hendelser. I den forbindelse bør vedkommende myndigheter og personvernmyndighetene samarbeide og utveksle opplysninger om alle forhold som er relevante for å håndtere eventuelle brudd på personopplysningssikkerheten som skjer som følge av hendelser.

64) Jurisdiksjonen over tilbydere av digital tjenester bør ligge hos den medlemsstaten der den aktuelle tilbyderen av digitale tjenester har sin hovedvirksomhet i Unionen, som i prinsippet svarer til det stedet der tilbyderens hovedkontor i Unionen ligger. Med virksomhet menes at det effektivt og faktisk utøves aktivitet gjennom en stabil struktur. En slik strukturs juridiske form, enten det dreier seg om en filial eller et datterforetak med status som juridisk person, er ikke den

avgjørende faktoren i den forbindelse. Dette kriteriet bør ikke avhenge av om nettverks- og informasjonssystemene er fysisk lokalisert på et bestemt sted. Det at slike systemer finnes og brukes, innebærer ikke i seg selv slik hovedvirksomhet og er derfor ikke kriterier for å fastslå hovedvirksomheten.

65) Når en tilbyder av digitale tjenester som ikke er etablert i Unionen, tilbyr tjenester i Unionen, bør den utpeke en representant. For å avgjøre om en slik tilbyder av digitale tjenester tilbyr tjenester i Unionen, bør det fastslås om det er åpenbart at tilbyderen av digitale tjenester har til hensikt å tilby tjenester til personer i en eller flere medlemsstater. Det forholdet at nettstedet til tilbyderen av digitale tjenester eller til en formidler, eller en e-postadresse og andre kontaktopplysninger, er tilgjengelige i Unionen, eller at det brukes et språk som vanligvis brukes i det tredjelandet der tilbyderen av digitale tjenester er etablert, er ikke i seg selv tilstrekkelig til å fastslå en slik hensikt. Imidlertid kan for eksempel bruk av et språk eller en valuta som vanligvis brukes i en eller flere medlemsstater, med mulighet til å bestille tjenester på det språket, eller omtale av kunder eller brukere i Unionen, gjøre det åpenbart at tilbyderen av digitale tjenester har til hensikt å tilby tjenester innenfor Unionen. Representanten bør handle på vegne av tilbyderen av digitale tjenester, og det bør være mulig for vedkommende myndigheter eller CSIRT-enhetene å kontakte representanten. Representanten bør utpekes uttrykkelig gjennom skriftlig fullmakt fra tilbyderen av digitale tjenester til å opptre på dennes vegne med hensyn til sistnevntes forpliktelser i henhold til dette direktivet, herunder rapportering av hendelser.

66) Standardisering av sikkerhetskrav er en markedsdrevet prosess. For å sørge for tilnærming i anvendelsen av sikkerhetsstandarder bør medlemsstatene oppmuntre til overholdelse av eller samsvar med nærmere angitte standarder, for på den måten å sikre et høyt sikkerhetsnivå i nettverks- og informasjonssystemer på unionsplan. ENISA bør bistå medlemsstatene med råd og retningslinjer. Det kan derfor være nyttig å utarbeide utkast til harmoniserte standarder, og dette bør gjøres i samsvar med europaparlaments- og rådsforordning (EU) nr. 1025/2012([8]).

67) Enheter som faller utenfor dette direktivets virkeområde, kan oppleve hendelser som har en betydelig innvirkning på de tjenestene de tilbyr. Dersom disse enhetene mener det er i offentlighetens interesse at de melder fra om slike hendelser, bør de kunne gjøre dette på frivillig grunnlag. Slike meldinger bør behandles av vedkommende myndighet eller CSIRT-enheten, forutsatt at behandlingen ikke utgjør en uforholdsmessig eller urimelig byrde for de berørte medlemsstatene.

68) For å sikre ensartede vilkår for gjennomføringen av dette direktivet bør Kommisjonen gis gjennomføringsmyndighet til å fastsette de saksbehandlingsreglene som er nødvendige for samarbeidsgruppens virksomhet, og de sikkerhets- og meldingskravene som skal gjelde for tilbydere av digitale tjenester. Denne myndigheten bør utøves i samsvar med europaparlaments- og rådsforordning (EU) nr. 182/2011([9]). Når Kommisjonen vedtar gjennomføringsrettsakter om de saksbehandlingsreglene som er nødvendige for samarbeidsgruppens virksomhet, bør den ta størst mulig hensyn til uttalelsen fra ENISA.

69) Når Kommisjonen vedtar gjennomføringsrettsakter om sikkerhetskravene til tilbydere av digitale tjenester, bør den ta størst mulig hensyn til uttalelsen fra ENISA og rådføre seg med berørte parter. I tillegg oppfordres Kommisjonen til å ta hensyn til følgende eksempler: når det gjelder sikkerhet for systemer og anlegg: fysisk og miljømessig sikkerhet, forsyningssikkerhet, kontroll av tilgang til nettverks- og informasjonssystemer og integriteten til nettverks- og informasjonssystemer; når det gjelder håndtering av hendelser: prosedyrer for hendelseshåndtering, kapasitet til å påvise hendelser, hendelsesrapportering og kommunikasjon; når det gjelder styring av driftskontinuitet: strategi for opprettholdelse av tjenester samt beredskapsplaner, kapasitet til gjenoppretting etter katastrofer; og når det gjelder overvåking, revisjon og testing: strategier for overvåking og loggføring, planer for beredskapsøvelser, testing av nettverks- og informasjonstjenester, sikkerhetsvurderinger og overvåking av samsvar.

70) Ved gjennomføringen av dette direktivet bør Kommisjonen ved behov ha kontakt med relevante sektorkomiteer og relevante organer som er opprettet på unionsplan på de områdene som omfattes av dette direktivet.

([8]) Europaparlaments- og rådsforordning (EU) nr. 1025/2012 av 25. oktober 2012 om europeisk standardisering og om endring av rådsdirektiv 89/686/EØF og 93/15/EØF samt europaparlaments- og rådsdirektiv 94/9/EF, 94/25/EF, 95/16/EF, 97/23/EF, 98/34/EF, 2004/22/EF, 2007/23/EF, 2009/23/EF og 2009/105/EF og om oppheving av rådsvedtak 87/95/EØF og europaparlaments- og rådsbeslutning nr. 1673/2006/EF (EUT L 316 av 14.11.2012, s. 12).

([9]) Europaparlaments- og rådsforordning (EU) nr. 182/2011 av 16. februar 2011 om fastsettelse av allmenne regler og prinsipper for medlemsstatenes kontroll med Kommisjonens utøvelse av sin gjennomføringsmyndighet (EUT L 55 av 28.2.2011, s. 13).

71) Kommisjonen bør med jevne mellomrom revidere dette direktivet i samråd med berørte parter, særlig for å avgjøre om det er nødvendig å endre det for å ta hensyn til endringer i de samfunnsmessige, politiske eller teknologiske vilkårene eller i markedsvilkårene.

72) Når opplysninger om risikoer og hendelser utveksles i samarbeidsgruppen og i nettverket av CSIRT-enheter, og ved overholdelse av kravet om å melde hendelser til vedkommende nasjonale myndigheter eller CSIRT-enhetene, kan det bli nødvendig å behandle personopplysninger. Slik behandling bør skje i samsvar med europaparlaments- og rådsdirektiv 95/46/EF([10]) og europaparlaments- og rådsforordning (EF) nr. 45/2001([11]). Ved anvendelsen av dette direktivet bør europaparlaments- og rådsforordning (EF) nr. 1049/2001([12]) få anvendelse i nødvendig omfang.

73) EUs datatilsyn ble rådspurt i samsvar med artikkel 28 nr. 2 i forordning (EF) nr. 45/2001 og avga uttalelse 14. juni 2013([13]).

74) Ettersom målet for dette direktivet, som er å oppnå et høyt felles nivå for sikkerhet i nettverks- og informasjonssystemer i Unionen, ikke kan nås i tilstrekkelig grad av medlemsstatene, men på grunn av tiltakets virkninger bedre kan nås på unionsplan, kan Unionen treffe tiltak i samsvar med nærhetsprinsippet som fastsatt i artikkel 5 i traktaten om Den europeiske union. I samsvar med forholdsmessighetsprinsippet fastsatt i nevnte artikkel, går dette direktivet ikke lenger enn det som er nødvendig for å nå dette målet.

75) Dette direktivet er forenlig med de grunnleggende rettighetene og de prinsippene som er anerkjent i Den europeiske unions pakt om grunnleggende rettigheter, særlig retten til respekt for privatliv og kommunikasjon, retten til vern av personopplysninger, friheten til å drive næringsvirksomhet, eiendomsretten, retten til effektiv klageadgang for en domstol og retten til å bli hørt. Dette direktivet bør gjennomføres i samsvar med nevnte rettigheter og prinsipper.

VEDTATT DETTE DIREKTIVET:

KAPITTEL I

ALMINNELIGE BESTEMMELSER

Artikkel 1

Formål og virkeområde

1. Dette direktivet fastsetter tiltak med sikte på å oppnå et høyt felles sikkerhetsnivå i nettverks- og informasjonssystemer i Unionen, for å forbedre det indre markeds funksjon.

2. For dette formålet blir det i dette direktivet

a) fastsatt at alle medlemsstater er forpliktet til å vedta en nasjonal strategi for sikkerhet i nettverks- og informasjonssystemer,

b) opprettet en samarbeidsgruppe med henblikk på å støtte og fremme strategisk samarbeid og utveksling av opplysninger mellom medlemsstatene og skape tillit og trygghet blant dem,

c) opprettet et nettverk av enheter for håndtering av digitale hendelser («CSIRT-nettverk») for å bidra til å skape tillit og trygghet blant medlemsstatene og for å fremme et raskt og effektivt driftsmessig samarbeid,

([10]) Europaparlaments- og rådsdirektiv 95/46/EF av 24. oktober 1995 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (EFT L 281 av 23.11.1995, s. 31).

([11]) Europaparlaments- og rådsforordning (EF) nr. 45/2001 av 18. desember 2000 om personvern i forbindelse med behandling av personopplysninger i Fellesskapets institusjoner og organer og om fri utveksling av slike opplysninger (EFT L 8 av 8.12.2001, s. 1).

([12]) Europaparlaments- og rådsforordning (EF) nr. 1049/2001 av 30. mai 2001 om offentlig tilgang til Europaparlamentets, Rådets og Kommisjonens dokumenter (EFT L 145 av 31.5.2001, s. 43).

([13]) EUT C 32 av 4.2.2014, s. 19.

d) fastsatt sikkerhets- og meldingskrav til ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester,

e) fastsatt at medlemsstatene er forpliktet til å utpeke vedkommende nasjonale myndigheter, felles kontaktpunkter og CSIRT-enheter, som pålegges oppgaver knyttet til sikkerhet i nettverks- og informasjonssystemer.

3. Sikkerhets- og meldingskravene i dette direktivet får ikke anvendelse på foretak som omfattes av kravene i artikkel 13a og 13b i direktiv 2002/21/EF, eller på ytere av tillitstjenester som omfattes av kravene i artikkel 19 i forordning (EU) nr. 910/2014.

4. Dette direktivet får anvendelse uten at det berører rådsdirektiv 2008/114/EF([14]) og europaparlaments- og rådsdirektiv 2011/93/EU([15]) og 2013/40/EU([16]).

5. Uten at det berører artikkel 346 i TEUV skal opplysninger som er fortrolige i henhold til Unionens og nasjonale regler, som for eksempel regler om forretningshemmeligheter, utveksles med Kommisjonen og andre relevante myndigheter bare dersom utvekslingen er nødvendig for anvendelsen av dette direktivet. Opplysningene som utveksles, skal være begrenset til det som er relevant, og som står i forhold til formålet med utvekslingen. Ved slik utveksling skal det sikres fortrolig behandling av opplysningene og vern av sikkerhets- og forretningsinteressene til ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester.

6. Dette direktivet berører ikke tiltak som medlemsstatene treffer for å ivareta sine grunnleggende statsfunksjoner, særlig for å ivareta nasjonal sikkerhet, herunder tiltak for å verne opplysninger hvis offentliggjøring etter medlemsstatenes syn vil stride mot deres vesentlige sikkerhetsinteresser, og for å opprettholde lov og orden, særlig for å muliggjøre etterforskning, avsløring og rettslig forfølging av straffbare forhold.

7. Dersom en sektorspesifikk unionsrettsakt inneholder krav om at ytere av samfunnsviktige tjenester eller tilbydere av digitale tjenester enten skal ivareta sikkerheten i sine nettverks- og informasjonssystemer eller melde fra om hendelser, forutsatt at disse kravene har minst tilsvarende virkning som forpliktelsene fastsatt i dette direktivet, får bestemmelsene i den sektorspesifikke unionsrettsakten anvendelse.

Artikkel 2

Behandling av personopplysninger

1. Behandling av personopplysninger i henhold til dette direktivet skal skje i samsvar med direktiv 95/46/EF.

2. Behandling av personopplysninger som utføres av Unionens institusjoner og organer i henhold til dette direktivet, skal skje i samsvar med forordning (EF) nr. 45/2001.

Artikkel 3

Minsteharmonisering

Uten at det berører artikkel 16 nr. 10 og medlemsstatenes forpliktelser i henhold til unionsretten, kan medlemsstatene vedta eller opprettholde bestemmelser med sikte på å oppnå et høyere sikkerhetsnivå i nettverks- og informasjonssystemer.

([14]) Rådsdirektiv 2008/114/EF av 8. desember 2008 om identifisering og utpeking av europeisk kritisk infrastruktur og vurdering av behovet for å beskytte den bedre (EUT L 345 av 23.12.2008, s. 75).

([15]) Europaparlaments- og rådsdirektiv 2011/93/EU av 13. desember 2011 om bekjempelse av seksuelt misbruk og seksuell utnytting av barn og barnepornografi, og om erstatning av Rådets rammebeslutning 2004/68/JIS (EUT L 335 av 17.12.2011, s. 1).

([16]) Europaparlaments- og rådsdirektiv 2013/40/EU av 12. august 2013 om angrep på informasjonssystemer, og om erstatning av Rådets rammebeslutning 2005/222/JIS (EUT L 218 av 14.8.2013, s. 8).

Artikkel 4

Definisjoner

I dette direktivet menes med

1) «nettverks- og informasjonssystem»

   a) et elektronisk kommunikasjonsnett som definert i artikkel 2 bokstav a) i direktiv 2002/21/EF,

   b) en innretning eller en gruppe innretninger som er koplet sammen eller hører sammen med hverandre, hvorav en eller flere av ved hjelp av et program utfører automatisk behandling av digitale data, eller

   c) digitale data som lagres, behandles, innhentes eller overføres med elementer som omfattes av bokstav a) og b), med henblikk på drift, bruk, vern og vedlikehold av disse,

2) «sikkerhet i nettverks- og informasjonsystemer» den evnen nettverks- og informasjonssystemer med en gitt grad av sikkerhet har til å motstå enhver handling som undergraver tilgjengeligheten, autentisiteten, integriteten eller fortroligheten av data som lagres, overføres eller behandles, eller de tilknyttede tjenestene som tilbys av eller er tilgjengelige via slike nettverks- og informasjonssystemer,

3) «nasjonal strategi for sikkerhet i nettverks- og informasjonssystemer» en ramme med strategiske mål og prioriteringer for sikkerhet i nettverks- og informasjonssystemer på nasjonalt plan,

4) «yter av samfunnsviktige tjenester» en offentlig eller privat enhet av en type nevnt i vedlegg II som oppfyller kriteriene fastsatt i artikkel 5 nr. 2,

5) «digital tjeneste» en tjeneste som definert i artikkel 1 nr. 1 bokstav b) i europaparlaments- og rådsdirektiv (EU) 2015/1535([17]) av en type som er oppført i vedlegg III,

6) «tilbyder av digitale tjenester» enhver juridisk person som tilbyr en digital tjeneste,

7) «hendelse» enhver inntruffet situasjon som har en faktisk negativ innvirkning på sikkerheten i nettverks- og informasjonssystemer,

8) «hendelseshåndtering» alle prosedyrer som støtter påvisning, analyse og begrensning av en hendelse samt all tilknyttet innsats,

9) «risiko» enhver rimelig identifiserbar omstendighet eller hendelse som har en potensiell negativ innvirkning på sikkerheten i nettverks- og informasjonssystemer,

10) «representant» enhver fysisk eller juridisk person etablert i Unionen som er uttrykkelig utpekt til å handle på vegne av en tilbyder av digitale tjenester som ikke er etablert i Unionen, og som vedkommende nasjonale myndighet eller en CSIRT-enhet kan henvende seg til i stedet for til tilbyderen av digitale tjenester angående de forpliktelsene som tilbyderen av digitale tjenester har i henhold til dette direktivet,

11) «standard» en standard som definert i artikkel 2 nr. 1 i forordning (EU) nr. 1025/2012,

12) «spesifikasjon» en teknisk spesifikasjon som definert i artikkel 2 nr. 4 i forordning (EU) nr. 1025/2012,

13) «samtrafikkpunkt på Internett (IXP)» en nettverksstruktur som gjør det mulig å kople sammen mer enn to uavhengige autonome systemer, hovedsakelig for å lette utveksling av internettrafikk; en IXP sørger bare for sammenkopling av autonome systemer; en IXP krever ikke at internettrafikk mellom to deltakende autonome systemer passerer gjennom et tredje autonomt system, og den endrer heller ikke slik trafikk eller forstyrrer den på annen måte,

14) «domenenavnsystem (DNS)» et hierarkisk oppbygd navngivingssystem i et nettverk som håndterer forespørsler om domenenavn,

([17]) Europaparlaments- og rådsdirektiv (EU) 2015/1535 av 9. september 2015 om en informasjonsprosedyre for tekniske forskrifter og regler for informasjonssamfunnstjenester (EUT L 241 av 17.9.2015, s. 1).

15) «tilbyder av DNS-tjenester» en enhet som tilbyr DNS-tjenester på internett,

16) «registerenhet for toppdomener» en enhet som forvalter og driver registreringen av internettdomenenavn under et bestemt toppdomene (TLD),

17) «nettbasert markedsplass» en digital tjeneste som gjør det mulig for forbrukere og/eller næringsdrivende som definert i henholdsvis bokstav a) og b) i artikkel 4 nr. 1 i europaparlaments- og rådsdirektiv 2013/11/EU([18]), å inngå nettbaserte salgs- eller tjenesteavtaler med næringsdrivende enten på nettstedet til den nettbaserte markedsplassen eller på en næringsdrivendes nettsted som bruker datatjenester som leveres av den nettbaserte markedsplassen,

18) «nettbasert søkemotor» et digital tjeneste som gjør det mulig for brukerne å foreta søk på i prinsippet alle nettsteder eller på nettsteder på et bestemt språk, på grunnlag av en forespørsel om et hvilket som helst emne i form av et søkeord, en søkefrase eller andre inndata, og som returnerer lenker til nettsider med informasjon om det forespurte innholdet,

19) «skytjeneste» en digital tjeneste som gir tilgang til en skalerbar og elastisk samling av delbare databehandlingsressurser.

Artikkel 5

Identifikasjon av ytere av samfunnsviktige tjenester

1. Innen 9. november 2018 skal medlemsstatene for hver sektor og delsektor som er nevnt i vedlegg II, identifisere de yterne av samfunnsviktige tjenester som er etablert på deres territorium.

2. Kriteriene for identifikasjon av ytere av samfunnsviktige tjenester i henhold til artikkel 4 nr. 4 skal være som følger:

a) En enhet yter en tjeneste som er avgjørende for å opprettholde kritisk samfunnsmessig og/eller økonomisk virksomhet.

b) Tjenesten avhenger av nettverks- og informasjonssystemer.

c) En hendelse vil ha en betydelig forstyrrende innvirkning på leveringen av tjenesten.

3. Med henblikk på nr. 1 skal hver medlemsstat utarbeide en liste over tjenestene nevnt i nr. 2 bokstav a).

4. Med henblikk på nr. 1, dersom en enhet leverer en tjeneste som nevnt i nr. 2 bokstav a) i to eller flere medlemsstater, skal disse medlemsstatene samrå seg med hverandre. Samrådet skal finne sted før det tas en beslutning om identifikasjon.

5. Medlemsstatene skal regelmessig og minst hvert andre år etter 9. mai 2018 revidere og om nødvendig ajourføre listen over identifiserte ytere av samfunnsviktige tjenester.

6. Samarbeidsgruppens rolle skal i samsvar med de oppgavene som er nevnt i artikkel 11, være å hjelpe medlemsstatene med å følge en konsekvent framgangsmåte i prosessen med å identifisere ytere av samfunnsviktige tjenester.

7. Med henblikk på revisjonen nevnt i artikkel 23 skal medlemsstatene innen 9. november 2018 og deretter hvert andre år sende Kommisjonen de opplysningene som er nødvendige for at den skal kunne vurdere gjennomføringen av dette direktivet, særlig konsekvensen i medlemsstatenes framgangsmåter for identifikasjon av ytere av samfunnsviktige tjenester. Opplysningene skal minst omfatte følgende:

a) nasjonale tiltak som gjør det mulig å identifisere ytere av samfunnsviktige tjenester,

([18]) Europaparlaments- og rådsdirektiv 2013/11/EU av 21. mai 2013 om alternativ tvisteløsning i forbrukersaker og om endring av forordning (EF) nr. 2006/2004 og direktiv 2009/22/EF (ATF-direktivet) (EUT L 165 av 18.6.2013, s. 63).

b) listen over tjenester nevnt i nr. 3,

c) antall ytere av samfunnsviktige tjenester som er identifisert for hver sektor nevnt i vedlegg II, med angivelse av deres betydning for sektoren,

d) terskelverdier, dersom slike finnes, for å bestemme det relevante forsyningsnivået ut fra antall brukere som er avhengige av tjenesten, i samsvar med artikkel 6 nr. 1 bokstav a), eller ut fra betydningen av den bestemte yteren av samfunnsviktige tjenester, i samsvar med artikkel 6 nr. 1 bokstav f).

For å bidra til at det leveres sammenlignbare opplysninger, kan Kommisjonen, under størst mulig hensyn til uttalelsen fra ENISA, vedta egnede tekniske retningslinjer om parametrene for de opplysningene som er omhandlet i dette nummeret.

Artikkel 6

Betydelig forstyrrende innvirkning

1. Når medlemsstatene skal fastslå betydningen av en forstyrrende innvirkning som nevnt i artikkel 5 nr. 2 bokstav c), skal de minst ta hensyn til følgende tverrsektorielle faktorer:

a) antall brukere som er avhengige av tjenesten som leveres av den aktuelle enheten,

b) hvor avhengige andre sektorer nevnt i vedlegg II er av tjenesten som leveres av enheten,

c) den innvirkningen, i form av omfang og varighet, som hendelser kan ha på økonomisk og samfunnsmessig virksomhet eller på offentlig sikkerhet,

d) enhetens markedsandel,

e) størrelsen på det geografiske området som kan bli berørt av en hendelse,

f) enhetens betydning for å opprettholde et tilstrekkelig tjenestenivå, tatt i betraktning tilgjengeligheten av alternative måter å få levert tjenesten på.

2. For å avgjøre om en hendelse kan ha en betydelig forstyrrende innvirkning, skal medlemsstatene også, når det er relevant, ta hensyn til sektorspesifikke faktorer.

KAPITTEL II

NASJONALE RAMMER FOR SIKKERHET I NETTVERKS- OG INFORMASJONSSYSTEMER

Artikkel 7

Nasjonal strategi for sikkerhet i nettverks- og informasjonssystemer

1. Hver medlemsstat skal vedta en nasjonal strategi for sikkerhet i nettverks- og informasjonssystemer som fastsetter strategiske mål og egnede politiske og lovgivningsmessige tiltak med sikte på å oppnå og opprettholde et høyt sikkerhetsnivå i nettverks- og informasjonssystemer, og som minst omfatter sektorene nevnt i vedlegg II og tjenestene nevnt i vedlegg III. Den nasjonale strategien for sikkerhet i nettverks- og informasjonssystemer skal særlig omfatte følgende:

a) målene og prioriteringene i den nasjonal strategien for sikkerhet i nettverks- og informasjonssystemer,

b) en forvaltningsramme for å nå målene og prioriteringene i den nasjonale strategien for sikkerhet i nettverks- og informasjonssystemer, herunder offentlige organers og andre relevante aktørers roller og ansvarsområder,

c) en liste over tiltak knyttet til beredskap, håndtering og gjenoppretting, herunder samarbeid mellom offentlig og privat sektor,

d) en angivelse av utdannings-, bevisstgjørings- og opplæringsprogrammer forbundet med den nasjonale strategien for sikkerhet i nettverks- og informasjonssystemer,

e) en angivelse av forsknings- og utviklingsplaner forbundet med den nasjonale strategien for sikkerhet i nettverks- og informasjonssystemer,

f) en risikovurderingsplan for å identifisere risikoer,

g) en liste over de ulike aktørene som deltar i gjennomføringen av den nasjonale strategien for sikkerhet i nettverks- og informasjonssystemer.

2. Medlemsstatene kan be om bistand fra ENISA ved utarbeidingen av nasjonale strategier for sikkerhet i nettverks- og informasjonssystemer.

3. Medlemsstatene skal underrette Kommisjonen om sine nasjonale strategier for sikkerhet nettverks- og informasjonssystemer innen tre måneder etter at de er vedtatt. I den forbindelse kan medlemsstatene utelate deler av strategien som gjelder nasjonal sikkerhet.

Artikkel 8

Vedkommende nasjonale myndigheter og et felles kontaktpunkt

1. Hver medlemsstat skal utpeke en eller flere vedkommende nasjonale myndigheter for sikkerhet i nettverks- og informasjonssystemer («vedkommende myndighet») som minst dekker sektorene nevnt i vedlegg II og tjenestene nevnt i vedlegg III. Medlemsstatene kan gi denne rollen til en eller flere eksisterende myndigheter.

2. Vedkommende myndigheter skal overvåke anvendelsen av dette direktivet på nasjonalt plan.

3. Hver medlemsstat skal utpeke et nasjonalt felles kontaktpunkt for sikkerhet i nettverks- og informasjonssystemer («felles kontaktpunkt»). Medlemsstatene kan gi denne rollen til en eksisterende myndighet. Dersom en medlemsstat utpeker bare én vedkommende myndighet, skal denne vedkommende myndigheten også være det felles kontaktpunktet.

4. Det felles kontaktpunktet skal fungere som et mellomledd for å sikre samarbeid over landegrensene mellom medlemsstatens myndigheter og de relevante myndighetene i andre medlemsstater, og med samarbeidsgruppen omhandlet i artikkel 11 og CSIRT-nettverket omhandlet i artikkel 12.

5. Medlemsstatene skal sikre at vedkommende myndigheter og de felles kontaktpunktene har tilstrekkelige ressurser til på en effektiv og formålstjenlig måte å utføre de oppgavene de blir pålagt, og dermed til å nå målene i dette direktivet. Medlemsstatene skal sikre at de utpekte representantene i samarbeidsgruppen samarbeider på en effektiv, formålstjenlig og sikker måte.

6. Vedkommende myndigheter og det felles kontaktpunktet skal, når det er hensiktsmessig og i samsvar med nasjonal rett, rådføre seg og samarbeide med de relevante nasjonale rettshåndhevende myndighetene og de nasjonale personvern-myndighetene.

7. Hver medlemsstat skal uten opphold underrette Kommisjonen om utpekingen av vedkommende myndighet og det felles kontaktpunktet samt om deres oppgaver og enhver senere endring av dem. Hver medlemsstat skal offentliggjøre utpekingen av vedkommende myndighet og det felles kontaktpunktet. Kommisjonen skal offentliggjøre listen over utpekte felles kontaktpunkter.

Artikkel 9

Enheter for håndtering av digitale hendelser (CSIRT-enheter)

1. Hver medlemsstat skal utpeke en eller flere CSIRT-enheter som skal oppfylle kravene i punkt 1 i vedlegg I, som minst dekker sektorene nevnt i vedlegg II og tjenestene nevnt i vedlegg III, og som har ansvar for å håndtere risikoer og hendelser i samsvar med en klart definert prosess. En CSIRT-enhet kan opprettes som en del av en vedkommende myndighet.

2. Medlemsstatene skal sikre at CSIRT-enhetene har tilstrekkelige ressurser til effektivt å utføre sine oppgaver, som er fastsatt i punkt 2 i vedlegg I.

Medlemsstatene skal sikre et effektivt, formålstjenlig og sikkert samarbeid mellom sine CSIRT-enheter og CSIRT-nettverket nevnt i artikkel 12.

3. Medlemsstatene skal sikre at deres CSIRT-enheter har tilgang til en egnet, sikker og robust kommunikasjons- og informasjonsinfrastruktur på nasjonalt plan.

4. Medlemsstatene skal underrette Kommisjonen om CSIRT-enhetenes oppgaver samt de viktigste elementene i CSIRT-enhetenes prosedyrer for hendelseshåndtering.

5. Medlemsstatene kan be om bistand fra ENISA til å opprette nasjonale CSIRT-enheter.

Artikkel 10

Samarbeid på nasjonalt plan

1. Dersom vedkommende myndighet, det felles kontaktpunktet og CSIRT-enheten i en medlemsstat er atskilte enheter, skal de samarbeide om å oppfylle forpliktelsene fastsatt i dette direktivet.

2. Medlemsstatene skal sikre at enten vedkommende myndigheter eller CSIRT-enhetene mottar hendelsesmeldinger som sendes inn i samsvar med dette direktivet. Dersom en medlemsstat beslutter at CSIRT-enheter ikke skal motta meldinger, skal CSIRT-enhetene, i den grad det er nødvendig for at de skal kunne utføre sine oppgaver, gis tilgang til data om hendelser som meldes inn av ytere av samfunnsviktige tjenester i samsvar med artikkel 14 nr. 3 og 5, eller av tilbydere av digitale tjenester i samsvar med artikkel 16 nr. 3 og 6.

3. Medlemsstatene skal sikre at vedkommende myndigheter eller CSIRT-enhetene underretter de felles kontaktpunktene om hendelsesmeldinger som sendes inn i samsvar med dette direktivet.

Innen 9. august 2018 og deretter hvert år skal det felles kontaktpunktet framlegge en sammenfattende rapport for samarbeidsgruppen om de mottatte meldingene, herunder antall meldinger og arten av de meldte hendelsene, og om tiltakene som er truffet i samsvar med artikkel 14 nr. 3 og 5 og artikkel 16 nr. 3 og 6.

KAPITTEL III

SAMARBEID

Artikkel 11

Samarbeidsgruppe

1. For å støtte og fremme strategisk samarbeid og utveksling av opplysninger mellom medlemsstatene og skape tillit og trygghet, og med sikte på å oppnå et høyt felles sikkerhetsnivå i nettverks- og informasjonssystemer i Unionen, opprettes det herved en samarbeidsgruppe.

Samarbeidsgruppen skal utføre sine oppgaver på grunnlag av toårige arbeidsprogrammer som nevnt i nr. 3 andre ledd.

2. Samarbeidsgruppen skal bestå av representanter for medlemsstatene, Kommisjonen og ENISA.

Når det er relevant, kan samarbeidsgruppen innby representanter for de berørte partene til å delta i dens arbeid.

Kommisjonen skal være sekretariat.

3. Samarbeidsgruppen skal ha følgende oppgaver:

a) gi strategisk veiledning om virksomheten i CSIRT-nettverket som er opprettet i henhold til artikkel 12,

b) utveksle beste praksis for utveksling av opplysninger angående melding av hendelser som nevnt i artikkel 14 nr. 3 og 5 og artikkel 16 nr. 3 og 6,

c) utveksle beste praksis mellom medlemsstatene og, i samarbeid med ENISA, bistå medlemsstatene i å bygge opp kapasitet for å ivareta sikkerheten i nettverks- og informasjonssystemer,

d) drøfte ressurser og beredskap i medlemsstatene og, på frivillig grunnlag, evaluere nasjonale strategier for sikkerhet i nettverks- og informasjonssystemer og CSIRT-enhetenes effektivitet, samt identifisere beste praksis,

e) utveksle opplysninger om og beste praksis for bevisstgjøring og opplæring,

f) utveksle opplysninger om og beste praksis for forskning og utvikling knyttet til sikkerhet i nettverks- og informasjonssystemer,

g) når det er relevant, utveksle erfaringer om spørsmål som gjelder sikkerheten i nettverks- og informasjonssystemer, med Unionens berørte institusjoner, organer, kontorer og byråer,

h) drøfte standardene og spesifikasjonene nevnt i artikkel 19 med representanter for de relevante europeiske standardiseringsorganisasjonene,

i) samle inn opplysninger om beste praksis i forbindelse med risikoer og hendelser,

j) undersøke, på årsbasis, de sammenfattende rapportene nevnt i artikkel 10 nr. 3 andre ledd,

k) drøfte arbeidet som er gjort med hensyn til øvelser knyttet til sikkerhet i nettverks- og informasjonssystemer, utdanningsprogrammer og opplæring, herunder det arbeidet som er utført av ENISA,

l) med ENISAs bistand utveksle beste praksis for medlemsstatenes identifikasjon av ytere av samfunnsviktige tjenester, også i forbindelse med grensekryssende avhengighetsforhold, når det gjelder risikoer og hendelser,

m) drøfte metoder for rapportering av hendelsesmeldinger som omhandlet i artikkel 14 og 16.

Innen 9. februar 2018 og deretter hvert andre år skal samarbeidsgruppen utarbeide et arbeidsprogram med tiltak som skal treffes for å gjennomføre dens mål og oppgaver, som skal være i samsvar med målene i dette direktivet.

4. Med henblikk på revisjonen nevnt i artikkel 23 skal samarbeidsgruppen innen 9. august 2018 og deretter hver 18. måned utarbeide en rapport om de erfaringene som er gjort ved det strategiske samarbeidet i henhold til denne artikkelen.

5. Kommisjonen skal vedta gjennomføringsrettsakter som fastsetter de saksbehandlingsreglene som er nødvendige for samarbeidsgruppens virksomhet. Disse gjennomføringsrettsaktene skal vedtas etter undersøkelsesprosedyren nevnt i artikkel 22 nr. 2.

Ved anvendelsen av første ledd skal Kommisjonen sende det første utkastet til gjennomføringsrettsakt til komiteen nevnt i artikkel 22 nr. 1 innen 9. februar 2017.

Artikkel 12

CSIRT-nettverk

1. For å bidra til å skape tillit blant medlemsstatene og fremme raskt og effektivt driftsmessig samarbeid opprettes det herved et nettverk av nasjonale CSIRT-enheter.

2. CSIRT-nettverket skal bestå av representanter for medlemsstatenes CSIRT-enheter og CERT-EU. Kommisjonen skal delta i CSIRT-nettverket som observatør. ENISA skal være sekretariat og skal aktivt støtte samarbeidet mellom CSIRT-enhetene.

3. CSIRT-nettverket skal ha følgende oppgaver:

a) utveksle opplysninger om CSIRT-enhetenes tjenester, drift og samarbeidsmuligheter,

b) på anmodning fra en CSIRT-representant for en medlemsstat som kan bli berørt av en hendelse, utveksle og drøfte ikke kommersielt følsomme opplysninger om hendelsen og risikoer forbundet med den; enhver medlemsstats CSIRT-enhet kan imidlertid nekte å bidra til disse drøftingene dersom det er fare for at det kan skade etterforskningen av hendelsen,

c) utveksle ikke-fortrolige opplysninger om enkelthendelser og på frivillig grunnlag gjøre slike opplysninger tilgjengelige,

d) på anmodning fra en representant for en medlemsstats CSIRT-enhet drøfte og om mulig finne fram til en samordnet innsats for å håndtere en hendelse som er blitt avdekket innenfor den medlemsstatens jurisdiksjon,

e) gi medlemsstatene støtte i håndteringen av grensekryssende hendelser på grunnlag av frivillig gjensidig bistand,

f) drøfte, undersøke og identifisere ytterligere former for driftsmessig samarbeid, herunder med hensyn til

   i) kategorier av risikoer og hendelser,

   ii) tidlige varslinger,

   iii) gjensidig bistand,

   iv) prinsipper og nærmere regler for samordning, når medlemsstatene setter inn tiltak mot grensekryssende risikoer og hendelser,

g) underrette samarbeidsgruppen om sin virksomhet og om ytterligere former for driftsmessig samarbeid som er drøftet i henhold til bokstav f), og be om veiledning om dette,

h) drøfte erfaringer fra øvelser vedrørende sikkerhet i nettverks- og informasjonssystemer, herunder fra øvelser som organiseres av ENISA,

i) på anmodning fra en gitt CSIRT-enhet drøfte denne CSIRT-enhetens ressurser og beredskap,

j) utarbeide retningslinjer for å fremme tilnærming i driftspraksis med hensyn til anvendelsen av bestemmelsene om driftsmessig samarbeid i denne artikkelen.

4. Med henblikk på revisjonen nevnt i artikkel 23 skal CSIRT-nettverket innen 9. august 2018 og deretter hver 18. måned utarbeide en rapport om de erfaringene som er gjort ved det driftsmessige samarbeidet i henhold til denne artikkelen, med konklusjoner og anbefalinger. Denne rapporten skal også sendes til samarbeidsgruppen.

5. CSIRT-nettverket skal fastsette sin egen forretningsorden.

Artikkel 13

Internasjonalt samarbeid

Unionen kan i samsvar med artikkel 218 i TEUV inngå internasjonale avtaler med tredjeland eller internasjonale organisasjoner for på den måten å tillate og legge til rette for at disse deltar i noen av samarbeidsgruppens aktiviteter. I slike avtaler skal det tas hensyn til behovet for å sikre tilstrekkelig vern av opplysninger.

KAPITTEL IV

SIKKERHET I NETTVERKS- OG INFORMASJONSSYSTEMER SOM BRUKES AV YTERE AV SAMFUNNSVIKTIGE TJENESTER

Artikkel 14

Sikkerhetskrav og melding av hendelser

1. Medlemsstatene skal sikre at ytere av samfunnsviktige tjenester treffer hensiktsmessige og forholdsmessige tekniske og organisatoriske tiltak for å håndtere risikoene knyttet til sikkerheten i de nettverks- og informasjonssystemene de bruker i sin virksomhet. I betraktning av det aktuelle tekniske utviklingstrinnet skal disse tiltakene garantere et sikkerhetsnivå i nettverks- og informasjonssystemer som står i forhold til risikoen.

2. Medlemsstatene skal sikre at ytere av samfunnsviktige tjenester treffer egnede tiltak for å forebygge og minimere innvirkningen av hendelser som påvirker sikkerheten i nettverks- og informasjonssystemer som brukes til å yte slike samfunnsviktige tjenester, med sikte på å sikre kontinuiteten i disse tjenestene.

3. Medlemsstatene skal sikre at ytere av samfunnsviktige tjenester uten unødig opphold melder fra til vedkommende myndighet eller CSIRT-enheten om hendelser som har en betydelig innvirkning på kontinuiteten i de samfunnsviktige tjenestene de yter. Meldingene skal inneholde opplysninger som gjør det mulig for vedkommende myndighet eller CSIRT-enheten å avgjøre om hendelsen har en innvirkning på tvers av landegrenser. Meldingen skal ikke innebære økt ansvar for melderen.

4. Med henblikk på å fastslå omfanget av en hendelses innvirkning skal det særlig tas hensyn til følgende parametrer:

a) antall brukere som er berørt av forstyrrelsen i den samfunnsviktige tjenesten,

b) hendelsens varighet,

c) størrelsen på det geografiske området som er berørt av hendelsen.

5. På grunnlag av opplysningene i meldingen fra yteren av samfunnsviktige tjenester skal vedkommende myndighet eller CSIRT-enheten underrette andre berørte medlemsstater dersom hendelsen har en betydelig innvirkning på kontinuiteten i samfunnsviktige tjenester i denne medlemsstaten. I den forbindelse skal vedkommende myndighet eller CSIRT-enheten, i samsvar med unionsretten eller nasjonal lovgivning som er forenlig med unionsretten, ivareta sikkerhets- og forretnings-interessene til yteren av samfunnsviktige tjenester og sikre fortrolig behandling av de opplysningene som gis i meldingen fra denne.

Når omstendighetene tillater det, skal vedkommende myndighet eller CSIRT-enheten gi den meldende yteren av samfunnsviktige tjenester relevante opplysninger om oppfølgingen av meldingen fra denne, for eksempel opplysninger som kan bidra til effektiv hendelseshåndtering.

På anmodning fra vedkommende myndighet eller CSIRT-enheten skal det felles kontaktpunktet videresende meldinger som nevnt i første ledd, til felles kontaktpunkter i andre berørte medlemsstater.

6. Etter å ha rådført seg med den meldende yteren av samfunnsviktige tjenester kan vedkommende myndighet eller CSIRT-enheten informere offentligheten om enkelthendelser dersom offentlighetens kjennskap til disse er nødvendig for å forebygge en hendelse eller håndtere en pågående hendelse.

7. Vedkommende myndigheter som agerer sammen innenfor samarbeidsgruppen, kan utarbeide og vedta retningslinjer om under hvilke omstendigheter ytere av samfunnsviktige tjenester er pålagt å melde hendelser, herunder parametrene for å fastsette omfanget av en hendelses innvirkning som nevnt i nr. 4.

Artikkel 15

Gjennomføring og håndheving

1. Medlemsstatene skal sikre at vedkommende myndigheter har de nødvendige fullmaktene og midlene til å vurdere om ytere av samfunnsviktige tjenester oppfyller sine forpliktelser i henhold til artikkel 14, og virkningene av dette på sikkerheten i nettverks- og informasjonssystemer.

2. Medlemsstatene skal sikre at vedkommende myndigheter har fullmakter og midler til å pålegge ytere av samfunnsviktige tjenester å levere

a) de opplysningene som er nødvendige for å vurdere sikkerheten i nettverks- og informasjonssystemene deres, herunder en dokumentert sikkerhetspolitikk,

b) bevis på effektiv gjennomføring av en sikkerhetspolitikk, for eksempel resultatene av en sikkerhetsrevisjon utført av vedkommende myndighet eller en kvalifisert inspektør og, i sistnevnte tilfelle, stille resultatene av denne og de underliggende bevisene til rådighet for vedkommende myndighet.

Når det anmodes om slike opplysninger eller bevis, skal vedkommende myndighet oppgi formålet med anmodningen og spesifisere hvilke opplysninger som kreves.

3. Etter vurderingen av opplysninger eller av resultatene fra sikkerhetsrevisjoner som nevnt i nr. 2, kan vedkommende myndighet gi bindende instrukser til ytere av samfunnsviktige tjenester om å avhjelpe de påviste manglene.

4. Vedkommende myndighet skal samarbeide tett med personvernmyndigheter når de håndterer hendelser som medfører brudd på personopplysningssikkerheten.

KAPITTEL V

SIKKERHET I NETTVERKS- OG INFORMASJONSSYSTEMER SOM BRUKES AV TILBYDERE AV DIGITALE TJENESTER

Artikkel 16

Sikkerhetskrav og melding av hendelser

1. Medlemsstatene skal sikre at tilbydere av digitale tjenester identifiserer og treffer hensiktsmessige og forholdsmessige tekniske og organisatoriske tiltak for å håndtere risikoene knyttet til sikkerheten i de nettverks- og informasjonssystemene de bruker i forbindelse med levering av tjenester nevnt i vedlegg III i Unionen. I betraktning av det aktuelle tekniske utviklingstrinnet skal disse tiltakene garantere et sikkerhetsnivå i nettverks- og informasjonssystemer som står i forhold til risikoen, og det skal tas hensyn til følgende elementer:

a) sikkerheten i systemer og anlegg,

b) hendelseshåndtering,

c) styring av driftskontinuitet,

d) overvåking, revisjon og testing,

e) overholdelse av internasjonale standarder.

2. Medlemsstatene skal sikre at tilbydere av digitale tjenester treffer tiltak for å forebygge og minimere den innvirkningen hendelser som påvirker sikkerheten i deres nettverks- og informasjonssystemer, har på tjenester nevnt i vedlegg III som tilbys i Unionen, med sikte på å sikre kontinuiteten i disse tjenestene.

3. Medlemsstatene skal sikre at tilbydere av digitale tjenester uten unødig opphold melder fra til vedkommende myndighet eller CSIRT-enheten om enhver hendelse som har en betydelig innvirkning på leveringen av en tjeneste nevnt i vedlegg III som de tilbyr i Unionen. Meldinger skal inneholde opplysninger som gjør det mulig for vedkommende myndighet eller CSIRT-enheten å fastslå omfanget av en eventuell innvirkning på tvers av landegrensene. Meldingen skal ikke innebære økt ansvar for melderen.

4. Med henblikk på å fastslå om innvirkningen av en hendelse er betydelig, skal det særlig tas hensyn til følgende parametrer:

a) antall brukere som er berørt av hendelsen, særlig brukere som er avhengige av tjenesten for å kunne levere egne tjenester,

b) hendelsens varighet,

c) størrelsen på det geografiske området som er berørt av hendelsen,

d) omfanget av driftsforstyrrelser i tjenesten,

e) omfanget av innvirkningen på økonomisk og samfunnsmessig virksomhet.

Plikten til å melde fra om en hendelse skal bare gjelde dersom tilbyderen av digitale tjenester har tilgang til de opplysningene som er nødvendige for å vurdere en hendelses innvirkning opp mot parametrene nevnt i første ledd.

5. Dersom en yter av samfunnsviktige tjenester er avhengig av en tredjepartstilbyder av digitale tjenester for å yte en tjeneste som er avgjørende for å opprettholde kritisk samfunnsmessig og økonomisk virksomhet, skal den tjenesteyteren melde fra om enhver betydelig innvirkning på kontinuiteten i den samfunnsviktige tjenesten som skyldes en hendelse som påvirker tilbyderen av digitale tjenester.

6. Dersom det er relevant, særlig dersom hendelsen nevnt i nr. 3 berører to eller flere medlemsstater, skal vedkommende myndighet eller CSIRT-enheten underrette de øvrige berørte medlemsstatene. I den forbindelse skal vedkommende myndigheter, CSIRT-enhetene og de felles kontaktpunktene, i samsvar med unionsretten eller nasjonal lovgivning som er forenlig med unionsretten, ivareta sikkerhets- og forretningsinteressene til tilbyderen av digitale tjenester og sikre fortrolig behandling av opplysningene som gis.

7. Etter å ha rådført seg med den berørte tilbyderen av digitale tjenester kan vedkommende myndighet eller CSIRT-enheten og, dersom det er relevant, myndighetene eller CSIRT-enhetene i andre berørte medlemsstater, informere offentligheten om enkelthendelser eller kreve at tilbyderen av digitale tjenester gjør det, dersom offentlighetens kjennskap til disse er nødvendig for å forebygge en hendelse eller håndtere en pågående hendelse, eller dersom det av andre grunner er i offentlighetens interesse at hendelsen gjøres kjent.

8. Kommisjonen skal vedta gjennomføringsrettsakter for ytterligere å spesifisere elementene nevnt i nr. 1 og parametrene nevnt i nr. 4 i denne artikkelen. Disse gjennomføringsrettsaktene skal vedtas etter undersøkelsesprosedyren nevnt i artikkel 22 nr. 2 innen 9. august 2017.

9. Kommisjonen kan vedta gjennomføringsrettsakter som fastsetter de formatene og prosedyrene som skal anvendes for å oppfylle meldingskravene. Disse gjennomføringsrettsaktene skal vedtas etter undersøkelsesprosedyren nevnt i artikkel 22 nr. 2.

10. Uten at det berører artikkel 1 nr. 6 skal medlemsstatene ikke pålegge tilbydere av digitale tjenester ytterligere sikkerhets- eller meldingskrav.

11. Kapittel V får ikke anvendelse på svært små og små bedrifter som definert i kommisjonsrekommandasjon 2003/361/EF([19]).

([19]) Kommisjonsrekommandasjon 2003/361/EF av 6. mai 2003 om definisjonen av svært små, små og mellomstore bedrifter (EFT L 124 av 20.5.2003, s. 36).

Artikkel 17

Gjennomføring og håndheving

1. Medlemsstatene skal sikre at vedkommende myndigheter ved behov griper inn gjennom tilsynstiltak i ettertid når det foreligger bevis på at en tilbyder av digitale tjenester ikke oppfyller kravene fastsatt i artikkel 16. Slike bevis kan sendes inn av en vedkommende myndighet i en annen medlemsstat der tjenesten leveres.

2. Med henblikk på nr. 1 skal vedkommende myndigheter ha de nødvendige fullmaktene og midlene til å pålegge tilbydere av digitale tjenester å

a) gi de opplysningene som er nødvendige for å vurdere sikkerheten i nettverks- og informasjonssystemene deres, herunder en dokumentert sikkerhetspolitikk,

b) avhjelpe enhver manglende oppfyllelse av kravene fastsatt i artikkel 16.

3. Dersom en tilbyder av digitale tjenester har sin hovedvirksomhet eller en representant i en medlemsstat, mens dens nettverks- og informasjonssystemer er lokalisert i en eller flere andre medlemsstater, skal vedkommende myndighet i hovedvirksomhetens eller representantens medlemsstat og vedkommende myndigheter i disse andre medlemsstatene samarbeide og bistå hverandre ved behov. Denne bistanden og dette samarbeidet kan omfatte utveksling av opplysninger mellom de berørte vedkommende myndighetene samt anmodninger om å treffe tilsynstiltakene nevnt i nr. 2.

Artikkel 18

Jurisdiksjon og territorialitetsprinsippet

1. Ved anvendelsen av dette direktivet skal en tilbyder av digitale tjenester anses å være underlagt jurisdiksjonen i den medlemsstaten der den har sin hovedvirksomhet. En tilbyder av digitale tjenester skal anses å ha sin hovedvirksomhet i en medlemsstat når den har sitt hovedkontor i den medlemsstaten.

2. En tilbyder av digitale tjenester som ikke er etablert i Unionen, men som tilbyr tjenester nevnt i vedlegg III i Unionen, skal utpeke en representant i Unionen. Representanten skal være etablert i en av de medlemsstatene der tjenestene tilbys. Tilbyderen av digitale tjenester skal anses å være underlagt jurisdiksjonen i den medlemsstaten der representanten er etablert.

3. At tilbyderen av digitale tjenester utpeker en representant, skal ikke berøre eventuelle rettslige skritt mot selve tilbyderen av digitale tjenester.

KAPITTEL VI

STANDARDISERING OG FRIVILLIG MELDING

Artikkel 19

Standardisering

1. For å fremme tilnærming i gjennomføringen av artikkel 14 nr. 1 og 2 og artikkel 16 nr. 1 og 2 skal medlemsstatene, uten å påby eller favorisere bruk av en bestemt type teknologi, oppmuntre til bruk av europeiske eller internasjonalt anerkjente standarder og spesifikasjoner som er relevante for sikkerheten i nettverks- og informasjonssystemer.

2. ENISA skal i samarbeid med medlemsstatene utarbeide råd og retningslinjer for de tekniske områdene som skal tas i betraktning i forbindelse med nr. 1, samt for eksisterende standarder som vil gjøre det mulig å dekke disse områdene, herunder medlemsstatenes nasjonale standarder.

Artikkel 20

Frivillig melding

1. Uten at det berører artikkel 3, kan enheter som ikke er blitt identifisert som ytere av samfunnsviktige tjenester, og som ikke er tilbydere av digitale tjenester, på frivillig grunnlag melde fra om hendelser som har en betydelig innvirkning på kontinuiteten i de tjenestene de yter.

2. Når medlemsstatene behandler meldinger, skal de handle i samsvar med prosedyren fastsatt i artikkel 14. Ved denne behandlingen kan medlemsstatene prioritere obligatoriske meldinger foran frivillige meldinger. Frivillige meldinger skal bare behandles når slik behandling ikke utgjør en uforholdsmessig eller urimelig byrde for medlemsstatene.

Frivillig melding skal ikke føre til at den meldende enheten pålegges noen forpliktelser som den ikke hadde vært omfattet av dersom den ikke hadde gitt denne meldingen.

KAPITTEL VII

SLUTTBESTEMMELSER

Artikkel 21

Sanksjoner

Medlemsstatene skal fastsette regler om sanksjoner for overtredelser av nasjonale bestemmelser som er vedtatt i henhold til dette direktivet, og skal treffe alle nødvendige tiltak for å sikre at de gjennomføres. Sanksjonene skal være virkningsfulle, stå i forhold til overtredelsen og virke avskrekkende. Medlemsstatene skal innen 9. mai 2018 underrette Kommisjonen om disse reglene og tiltakene og uten opphold underrette den om eventuelle senere endringer av dem.

Artikkel 22

Komitéframgangsmåte

1. Kommisjonen skal bistås av komiteen for sikkerhet i nettverks- og informasjonssystemer. Nevnte komité skal være en komité i henhold til forordning (EU) nr. 182/2011.

2. Når det vises til dette nummeret, får artikkel 5 i forordning (EU) nr. 182/2011 anvendelse.

Artikkel 23

Revisjon

1. Innen 9. mai 2019 skal Kommisjonen framlegge en rapport for Europaparlamentet og Rådet med en vurdering av konsekvensen i den framgangsmåten som medlemsstatene har fulgt ved identifikasjonen av av ytere av samfunnsviktige tjenester.

2. Kommisjonen skal regelmessig revidere virkningen av dette direktivet og framlegge en rapport for Europaparlamentet og Rådet. For dette formålet og for å fremme det strategiske og driftsmessige samarbeidet ytterligere skal Kommisjonen ta hensyn til rapportene fra samarbeidsgruppen og CSIRT-nettverket om de erfaringene som er gjort på strategisk og driftsmessig plan. Ved sin revisjon skal Kommisjonen også vurdere listene i vedlegg II og III samt konsekvensen i identifikasjonen av ytere av samfunnsviktige tjenester og av tjenester i sektorene nevnt i vedlegg II. Den første rapporten skal framlegges innen 9. mai 2021.

Artikkel 24

Overgangsbestemmelser

1. Uten at det berører artikkel 25, og for å gi medlemsstatene ytterligere muligheter til passende samarbeid mens innarbeidingen i nasjonal lovgivning pågår, skal samarbeidsgruppen og CSIRT-nettverket begynne å utføre oppgavene fastsatt i henholdsvis artikkel 11 nr. 3 og artikkel 12 nr. 3 innen 9. februar 2017.

2. I perioden fra 9. februar 2017 til 9. november 2018, for å hjelpe medlemsstatene å følge en konsekvent framgangsmåte i prosessen med å identifisere ytere av samfunnsviktige tjenester, skal samarbeidsgruppen drøfte prosedyren for, innholdet i og typen av nasjonale tiltak som gjør det mulig å identifisere ytere av samfunnsviktige tjenester i en bestemt sektor i samsvar med kriteriene i artikkel 5 og 6. På anmodning fra en medlemsstat skal samarbeidsgruppen også drøfte denne medlemsstatens utkast til særlige nasjonale tiltak som gjør det mulig å identifisere ytere av samfunnsviktige tjenester i en bestemt sektor i samsvar med kriteriene i artikkel 5 og 6.

3. Innen 9. februar 2017 og ved anvendelse av denne artikkelen skal medlemsstatene sikre hensiktsmessig representasjon i samarbeidsgruppen og CSIRT-nettverket.

Artikkel 25

Innarbeiding i nasjonal lovgivning

1. Medlemsstatene skal innen 9. mai 2018 vedta og kunngjøre de lovene og forskriftene som er nødvendige for å etterkomme dette direktivet. De skal umiddelbart underrette Kommisjonen om dette.

De skal anvende disse bestemmelsene fra 10. mai 2018.

Når disse bestemmelsene vedtas av medlemsstatene, skal de inneholde en henvisning til dette direktivet, eller det skal vises til direktivet når de kunngjøres. Nærmere regler for henvisningen fastsettes av medlemsstatene.

2. Medlemsstatene skal oversende Kommisjonen teksten til de viktigste internrettslige bestemmelsene som de vedtar på det området dette direktivet omhandler.

Artikkel 26

Ikrafttredelse

Dette direktivet trer i kraft den 20. dagen etter at det er kunngjort i *Den europeiske unions tidende*.

Artikkel 27

Adressater

Dette direktivet er rettet til medlemsstatene.

Utferdiget i Strasbourg 6. juli 2016.

For Europaparlamentet	*For Rådet*
M. SCHULZ	I. KORČOK
President	*Formann*

VEDLEGG I

KRAV TIL ENHETER FOR HÅNDTERING AV DIGITALE HENDELSER (CSIRT-ENHETER) OG DERES OPPGAVER

Kravene til CSIRT-enheter og deres oppgaver skal være tilstrekkelig og tydelig definert og skal være underbygd av nasjonal politikk og/eller lovgivning. De skal omfatte følgende:

1) Krav til CSIRT-enheter:

   a) CSIRT-enheter skal sikre at deres kommunikasjonstjenester har høy grad av tilgjengelighet ved å unngå svake punkter («single points of failure»), og skal til enhver tid og på flere måter kunne kontaktes og kunne kontakte andre. Dessuten skal kommunikasjonskanalene være tydelig angitt og godt kjent for brukergruppen og samarbeidspartnere.

   b) CSIRT-enhetenes lokaler og de underliggende informasjonssystemene skal være plassert på sikre steder.

   c) Driftskontinuitet:

      i) CSIRT-enheter skal være utstyrt med et egnet system for håndtering og videreformidling av anmodninger med henblikk på å lette overleveringer.

      ii) CSIRT-enheter skal ha tilstrekkelig personale til å sikre tilgjengelighet hele døgnet.

      iii) CSIRT-enheter skal ha en infrastruktur med garantert kontinuerlig drift. For dette formålet skal det finnes redundante systemer og reservearbeidsområder.

   d) CSIRT-enheter skal ha mulighet til å delta i internasjonale samarbeidsnettverk dersom de ønsker det.

2) CSIRT-enhetenes oppgaver:

   a) CSIRT-enhetenes oppgaver skal minst omfatte følgende:

      i) overvåking av hendelser på nasjonalt plan,

      ii) tidlig varsling, alarmer, meldinger og formidling av opplysninger til berørte parter om risikoer og hendelser,

      iii) iverksetting av tiltak ved hendelser,

      iv) dynamisk risiko- og hendelsesanalyse og situasjonsforståelse,

      v) deltakelse i CSIRT-nettverket.

   b) CSIRT-enheter skal inngå samarbeid med privat sektor.

   c) For å legge til rette for samarbeid skal CSIRT-enheter fremme vedtakelse og bruk av en felles eller standardisert praksis for

      i) hendelses- og risikohåndteringsprosedyrer og

      ii) klassifiseringssystemer for hendelser, risikoer og opplysninger.

———

VEDLEGG II

TYPER AV ENHETER MED HENBLIKK PÅ ARTIKKEL 4 NR. 4

Sektor	Delsektor	Type enhet
1. Energi	a) Elektrisitet	– Elektrisitetsforetak som definert i artikkel 2 nr. 35 i europaparlaments- og rådsdirektiv 2009/72/EF([1]) som ivaretar «forsyning» som definert i artikkel 2 nr. 19 i samme direktiv
		– Operatører av distribusjonsnett som definert i artikkel 2 nr. 6 i direktiv 2009/72/EF
		– Operatører av transmisjonsnett som definert i artikkel 2 nr. 4 i direktiv 2009/72/EF
	b) Olje	– Operatører av oljerørledninger
		– Operatører av anlegg for produksjon, raffinering, behandling, lagring og transmisjon av olje
	c) Gass	– Forsyningsforetak som definert i artikkel 2 nr. 8 i europaparlaments- og rådsdirektiv 2009/73/EF([2])
		– Operatører av distribusjonsnett som definert i artikkel 2 nr. 6 i direktiv 2009/73/EF
		– Operatører av transmisjonsnett som definert i artikkel 2 nr. 4 i direktiv 2009/73/EF
		– Operatører av lagringsanlegg som definert i artikkel 2 nr. 10 i direktiv 2009/73/EF
		– Operatører av LNG-nett som definert i artikkel 2 nr. 12 i direktiv 2009/73/EF
		– Naturgassforetak som definert i artikkel 2 nr. 1 i direktiv 2009/73/EF
		– Operatører av raffinerings- og behandlingsanlegg for naturgass
2. Transport	a) Lufttransport	– Luftfartsselskaper som definert i artikkel 3 nr. 4 i europaparlaments- og rådsforordning (EF) nr. 300/2008([3])
		– Lufthavnadministrasjoner som definert i artikkel 2 nr. 2 i europaparlaments- og rådsdirektiv 2009/12/EF([4]), lufthavner som definert i artikkel 2 nr. 1 i samme direktiv, herunder hovedlufthavnene oppført i avsnitt 2 i vedlegg II til europaparlaments- og rådsforordning (EU) nr. 1315/2013([5]), og foretak som driver tilhørende anlegg i lufthavner

Sektor	Delsektor	Type enhet
		– Operatører innen trafikkstyring som yter flygekontrolltjenester (ATC) som definert i artikkel 2 nr. 1 i europaparlaments- og rådsforordning (EF) nr. 549/2004([6])
	b) Jernbanetransport	– Infrastrukturforvaltere som definert i artikkel 3 nr. 2 i europaparlaments- og rådsdirektiv 2012/34/EU([7])
		– Jernbaneforetak som definert i artikkel 3 nr. 1 i direktiv 2012/34/EU, herunder operatører av serviceanlegg som definert i artikkel 3 nr. 12 i direktiv 2012/34/EU
	c) Transport på vannveier	– Foretak som driver passasjertrafikk og godstransport på innlands vannveier, til sjøs og langs kysten, i samsvar med definisjonen av sjøtransport i vedlegg I til europaparlaments- og rådsforordning (EF) nr. 725/2004([8]), med unntak av de enkelte fartøyene som drives av disse foretakene
		– Administrasjoner i havner som definert i artikkel 3 nr. 1 europaparlaments- og rådsdirektiv 2005/65/EF([9]), herunder havneanlegg som definert i artikkel 2 nr. 11 i forordning (EF) nr. 725/2004, samt foretak som driver anlegg og utstyr i havner
		– Operatører av sjøtrafikksentraler som definert i artikkel 3 bokstav o) i europaparlaments- og rådsdirektiv 2002/59/EF([10])
	d) Veitransport	– Veimyndigheter som definert i artikkel 2 nr. 12 i delegert kommisjonsforordning (EU) 2015/962([11]) med ansvar for trafikkstyring
		– Operatører av intelligente transportsystemer som definert i artikkel 4 nr. 1 i europaparlaments- og rådsdirektiv 2010/40/EU([12])
3. Bankvirksomhet		– Kredittinstitusjoner som definert i artikkel 4 nr. 1 i europaparlaments- og rådsforordning (EU) nr. 575/2013([13])
4. Finansmarkeds-infrastrukturer		– Operatører av handelsplasser som definert i artikkel 4 nr. 24 i europaparlaments- og rådsdirektiv 2014/65/EU([14])
		– Sentrale motparter som definert i artikkel 2 nr. 1 i europaparlaments- og rådsforordning (EU) nr. 648/2012([15])
5. Helsesektoren	Helsetjenestemiljøer (herunder sykehus og private klinikker)	– Helsetjenesteytere som definert i artikkel 3 bokstav g) i europaparlaments- og rådsdirektiv 2011/24/EU([16])

Sektor	Delsektor	Type enhet
6. Forsyning og distribusjon av drikkevann		Leverandører og distributører av drikkevann som definert i artikkel 2 nr. 1 bokstav a) i rådsdirektiv 98/83/EF([17]), men unntatt distributører hvis distribusjon av drikkevann bare utgjør en del av deres generelle virksomhet, som består av distribusjon av andre råvarer og varer, og som ikke anses som samfunnsviktige tjenester
7. Digital infrastruktur		– IXP-er
		– Tilbydere av DNS-tjenester
		– Registerenheter for toppdomener

([1]) Europaparlaments- og rådsdirektiv 2009/72/EF av 13. juli 2009 om felles regler for det indre marked for elektrisk kraft og om oppheving av direktiv 2003/54/EF (EUT L 211 av 14.8.2009, s. 55).
([2]) Europaparlaments- og rådsdirektiv 2009/73/EF av 13. juli 2009 om felles regler for det indre marked for naturgass og om oppheving av direktiv 2003/55/EF (EUT L 211 av 14.8.2009, s. 94).
([3]) Europaparlaments- og rådsforordning (EF) nr. 300/2008 av 11. mars 2008 om felles bestemmelser om sikkerhet i sivil luftfart og om oppheving av forordning (EF) nr. 2320/2002 (EUT L 97 av 9.4.2008, s. 72).
([4]) Europaparlaments- og rådsdirektiv 2009/12/EF av 11. mars 2009 om lufthamnavgifter (EUT L 70 av 14.3.2009, s. 11).
([5]) Europaparlaments- og rådsforordning (EU) nr. 1315/2013 av 11. desember 2013 om unionsretningslinjer for utviklingen av et transeuropeisk transportnett og om oppheving av beslutning nr. 661/2010/EU (EUT L 348 av 20.12.2013, s. 1).
([6]) Europaparlaments- og rådsforordning (EF) nr. 549/2004 av 10. mars 2004 om fastsettelse av rammeregler for opprettelse av et felles europeisk luftrom (rammeforordningen) (EUT L 96 av 31.3.2004, s. 1).
([7]) Europaparlaments- og rådsdirektiv 2012/34/EF av 21. november 2012 om opprettelse av et felles europeisk jernbaneområde (EUT L 343 av 14.3.2009, s. 32).
([8]) Europaparlaments- og rådsforordning (EF) nr. 725/2004 av 31. mars 2004 om forbedret sikkerhet for fartøyer og havneanlegg (EUT L 129 av 29.4.2004, s. 6).
([9]) Europaparlaments- og rådsdirektiv 2005/65/EF av 26. oktober 2005 om forbedret sikkerhet for havner (EUT L 310 av 25.11.2005, s. 28).
([10]) Europaparlaments- og rådsdirektiv 2002/59/EF av 27. juni 2002 om opprettelse av et overvåkings- og informasjonssystem for sjøtrafikk i Fellesskapet og om oppheving av rådsdirektiv 93/75/EØF (EFT L 208 av 5.8.2002, s. 10).
([11]) Delegert kommisjonsforordning (EU) nr. 2015/962 av 18. desember 2014 om utfylling av europaparlaments- og rådsdirektiv 2010/40/EU med hensyn til sanntids trafikkinformasjonstjenester på EU-plan (EUT L 157 av 23.6.2015, s 21).
([12]) Europaparlaments- og rådsdirektiv 2010/40/EU av 7. juli 2010 om en ramme for innføring av intelligente transportsystemer innen veitransport og for grensesnitt mot andre transportsystemer (EUT L 207 av 6.8.2010, s. 1).
([13]) Europaparlaments- og rådsforordning (EU) nr. 575/2013 av 26. juni 2013 om tilsynskrav for kredittinstitusjoner og verdipapirforetak og om endring av forordning (EU) nr. 648/2012 (EUT L 176 av 27.6.2013, s. 1).
([14]) Europaparlaments- og rådsdirektiv 2014/65/EU av 15. mai 2014 om markeder for finansielle instrumenter og om endring av direktiv 2002/92/EF og direktiv 2011/61/EU (EUT L 173 av 12.6.2014, s. 349).
([15]) Europaparlaments- og rådsforordning (EU) nr. 648/2012 av 4. juli 2012 om OTC-derivater, sentrale motparter og transaksjonsregistre (EUT L 201 av 27.7.2012, s. 1).
([16]) Europaparlaments- og rådsdirektiv 2011/24/EU av 9. mars 2011 om anvendelse av pasientrettigheter ved helsetjenester over landegrensene (EUT L 88 av 4.4.2011, s. 45).
([17]) Rådsdirektiv 98/83/EF av 3. november 1998 om drikkevannets kvalitet (EFT L 330 av 5.12.1998, s. 32).

VEDLEGG III

TYPER AV DIGITALE TJENESTER MED HENBLIKK PÅ ARTIKKEL 4 NR. 5

1. Nettbasert markedsplass.
2. Nettbasert søkemotor.
3. Skytjeneste.