DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

UOFFISIELL OVERSETTELSE

EUROPAPARLAMENTS- OG RÅDSDIREKTIV (EU) 2016/1148

av 6. juli 2016

om tiltak for å sikre et høyt felles nivå for sikkerhet i nett- 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) Nett- og informasjonssystemer og nett- og informasjonstjenester har en viktig rolle i samfunnet. Deres pålitelighet og sikkerhet er grunnleggende for økonomisk og samfunnsmessig virksomhet, og særlig for det indre markeds virkemåte.

2) Omfanget, hyppigheten og virkningen av sikkerhetshendelser er økende og utgjør en alvorlig trussel mot virkemåten til nett- og informasjonssystemer. Disse systemene kan også bli mål for tilsiktede skadelige handlinger beregnet på å skade eller forstyrre driften av systemene. Slike hendelser kan være til hinder for utøvelse av økonomisk virksomhet, skape betydelige økonomiske tap, undergrave brukernes tillit og få store negative konsekvenser for Unionens økonomi.

3) Nett- og informasjonssystemer, særlig Internett, er grunnleggende for å gjennomføre bevegelighet over landegrensene for varer, tjenester og personer. På grunn av det tverrnasjonale aspektet kan betydelige forstyrrelser i disse systemene, enten de er tilsiktet eller utilsiktet og uansett hvor de finner sted, påvirke de enkelte medlemsstatene og Unionen som helhet. Sikkerheten i nett- og informasjonssystemer er derfor avgjørende for et velfungerende indre marked.

4) På grunnlag av den store framdriften innenfor det europeiske forum for medlemsstater med hensyn til å fremme drøftinger og utveksling av god praksis, herunder utarbeiding av prinsipper for et europeisk samarbeid i tilfelle datarelaterte kriser, bør det opprettes en samarbeidsgruppe bestående av representanter for medlemsstatene, Kommisjonen og Den europeiske unions byrå for nett- og informasjonssikkerhet («ENISA») for å støtte og lette strategisk samarbeid mellom medlemsstatene om sikkerhet i nett- og informasjonssystemer. For at gruppen skal være effektiv og inkluderende, er det viktig at alle medlemsstater oppfyller et minstekrav til ressurser og har en strategi som sikrer et høyt nivå for sikkerhet i nett- og informasjonssystemer på eget territorium. I tillegg bør ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester være underlagt sikkerhets- og meldingskrav med

([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).

UOFFISIELL OVERSETTELSE

henblikk på å fremme en kultur for risikohåndtering og sikre rapportering av de mest alvorlige hendelsene.

5) De eksisterende ressursene er ikke tilstrekkelige til å sikre et høyt nivå for sikkerhet i nett- og informasjonssystemene i Unionen. Medlemsstatene har svært ulike beredskapsnivåer, noe som har ført til en usammenhengende tilnærming i hele Unionen. Dette fører til ulike vernenivåer for forbrukere og foretak, og undergraver det generelle nivået for sikkerhet i nett- 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 opprette en global og effektiv ordning for samarbeid på unionsplan. Universiteter og forskningssentre er avgjørende for å anspore til forskning, utvikling og innovasjon på disse områdene.

6) Effektive tiltak for å løse utfordringer knyttet til sikkerhet i nett- og informasjonssystemer krever derfor en global tilnærming på unionsplan som omfatter felles minstekrav til kapasitetsoppbygging og planlegging, utveksling av opplysninger, 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 er fastsatt i dette direktiv.

7) For å dekke alle relevante hendelser og risikoer bør dette direktiv få anvendelse på både 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 få anvendelse på foretak som leverer offentlige kommunikasjonsnett eller offentlig tilgjengelige elektroniske kommunikasjonstjenester i henhold til europaparlaments- og rådsdirektiv 2002/21/EF([3]), som omfattes av de særlige kravene til sikkerhet og integritet som er fastsatt i nevnte direktiv, og heller ikke på ytere av tillitstjenester i henhold til europaparlaments- og rådsforordning (EU) nr. 910/2014([4]), som omfattes av sikkerhetskravene fastsatt i nevnte forordning.

8) Dette direktiv bør ikke berøre muligheten hver enkelt medlemsstat har til å treffe nødvendige tiltak for å sikre vern av grunnleggende sikkerhetsinteresser, opprettholde offentlig orden og sikkerhet samt muliggjøre etterforskning, avsløring og rettslig forfølging av straffbare handlinger. 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. I denne sammenheng er rådsbeslutning 2013/488/EU([5]) og avtaler om taushetsplikt eller uformelle avtaler om taushetsplikt, som «Traffic Light Protocol», relevante.

9) Visse økonomiske sektorer er allerede regulert eller kan reguleres i framtiden ved sektorspesifikke unionsrettsakter som omfatter regler knyttet til sikkerhet i nett- og informasjonssystemer. Når disse unionsrettsaktene inneholder bestemmelser om innføring av krav til sikkerhet i nett- og informasjonssystemer eller meldinger om hendelser, bør disse bestemmelsene få anvendelse dersom de inneholder krav som i praksis minst tilsvarer forpliktelsene i dette direktiv. Medlemsstatene bør i så fall anvende bestemmelsene i slike sektorspesifikke unionsrettsakter, herunder bestemmelser som berører jurisdiksjon, og bør ikke gjennomføre identifikasjonsprosessen for ytere av samfunnsviktige tjenester som definert i dette direktiv. I den forbindelse bør medlemsstatene gi Kommisjonen opplysninger om anvendelsen av slike *lex specialis*. For å avgjøre om kravene til sikkerhet i nett- og informasjonssystemer og meldinger om hendelser som inngår i sektorspesifikke unionsrettsakter, tilsvarer dem som er fastsatt i dette direktiv, bør det tas hensyn bare til bestemmelsene i relevante unionsrettsakter og deres anvendelse i medlemsstatene.

10) I sektoren for transport på vannveier omfatter sikkerhetskravene til rederier, fartøyer, havneanlegg, havner og sjøtrafikksentraler i henhold til unionsrettsakter all virksomhet, herunder radio- og telekommunikasjonsutstyr, datasystemer og nett. De obligatoriske prosedyrene som skal følges, omfatter blant annet rapportering av alle hendelser, og bør derfor anses som *lex specialis*, i den utstrekning disse kravene minst tilsvarer de tilsvarende bestemmelsene i dette direktiv.

11) Når medlemsstatene identifiserer operatører i sektoren for transport på vannveier, bør de ta hensyn til eksisterende og kommende internasjonale regler og retningslinjer utarbeidet særlig av Den internasjonale sjøfartsorganisasjon, med sikte på å skape en enhetlig tilnærming for individuelle sjøtransportoperatører.

12) Regulering av og tilsyn med sektorene for bankvirksomhet og infrastrukturer i finansmarkedene er svært harmonisert på unionsplan gjennom Unionens primærrett og avledet regelverk samt standarder utviklet i samarbeid med de europeiske tilsynsmyndighetene. Innenfor bankunionen sikres anvendelsen og tilsynet med disse kravene gjennom den felles

([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).

UOFFISIELL OVERSETTELSE

tilsynsordningen. For medlemsstater som ikke er en del av bankunionen, sikres dette av medlemsstatenes relevante banktilsynsmyndigheter. På andre områder av tilsynet med finanssektoren bidrar også Det europeiske finanstilsynssystem til å sikre en høy grad av ensartethet og sammenfall i tilsynspraksis. Den europeiske verdipapir- og markedstilsynsmyndighet fører også direkte tilsyn med visse foretak, nærmere bestemt kredittvurderingsbyråer og transaksjonsregistre.

13) Operasjonell risiko er en viktig del av reguleringen av og tilsynet med sektorene for bankvirksomhet og infrastrukturer i finansmarkedet. Den omfatter all virksomhet, herunder nett- og informasjonssystemers sikkerhet, funksjonsdyktighet og robusthet. Kravene til disse systemene, som ofte går lenger enn kravene fastsatt i dette direktiv, er fastsatt i en rekke unionsrettsakter, herunder regler for adgang til å utøve virksomhet som kredittinstitusjon og tilsyn med kredittinstitusjoner og verdipapirforetak samt regler for tilsynskrav for kredittinstitusjoner og verdipapirforetak, som omfatter krav med hensyn til operasjonell risiko, regler for markeder for finansielle instrumenter, som omfatter krav med hensyn til risikovurdering for verdipapirforetak og for regulerte markeder, regler for OTC-derivater, sentrale motparter og transaksjonsregistre, som omfatter krav med hensyn til operasjonell risiko for sentrale motparter og transaksjonsregistre, og regler for forbedring av oppgjørssystemet for verdipapirer i Unionen og om verdipapirsentraler, som omfatter krav med hensyn til operasjonell risiko. Videre er krav til melding om hendelser en del av vanlig tilsynspraksis i finanssektoren og inngår ofte i tilsynshåndbøker. Medlemsstatene bør vurdere disse reglene og kravene i sin søknad om *lex specialis*.

14) Som Den europeiske sentralbank bemerker i sin uttalelse av 25. juli 2014([6]) berører ikke dette direktiv ordningen som er fastsatt i unionsretten for Eurosystemets tilsyn med betalings- og oppgjørssystemer. Det vil være hensiktsmessig for myndigheter med ansvar for slikt tilsyn å utveksle erfaringer om spørsmål som gjelder sikkerhet i nett- og informasjonssystemer, med vedkommende myndigheter i henhold til dette direktiv. Det samme gjelder for medlemmer i Det europeiske system av sentralbanker som står utenfor euroområdet og som fører slikt tilsyn med betalings- og oppgjørssystemer på grunnlag av 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 fungerer bare som en formidler av tredjemannstjenester hvor det er mulig å inngå en avtale i siste instans. Den bør derfor ikke omfatte nettbaserte tjenester som sammenligner prisen 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, sammenslåing av data eller profilering av brukere. Programbutikker, som fungerer som nettbutikker med henblikk på digital distribusjon av programmer eller programvare fra tredjemann, skal anses som en type nettbasert markedsplass.

16) En nettbasert søkemotor gjør det i prinsippet mulig for brukeren å foreta søk på alle nettsteder på grunnlag av et søk innenfor et hvilket som helst emne. Den kan også være rettet mot nettsteder på et bestemt språk. Definisjonen av en nettbasert søkemotor som er fastsatt i dette direktiv, 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 prisen 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. Med henblikk på dette direktiv omfatter «skytjenester» tjenester som gir tilgang til en skalerbar og fleksibel samling av delbare databehandlingsressurser. Disse databehandlingsressursene omfatter ressurser som nett, servere eller annen infrastruktur, lagring, programmer og tjenester. Begrepet «skalerbar» henspiller på databehandlingsressurser som tilbyderen av skytjenester fordeler på en fleksibel måte, uavhengig av ressursenes geografiske plassering, for å håndtere svingninger i etterspørselen. Begrepet «fleksibel samling» brukes til å beskrive databehandlingsressurser som stilles til rådighet og utnyttes avhengig av etterspørsel, slik at tilgjengelige ressurser 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 hvor databehandlingen foretas separat for hver enkelt bruker, selv om tjenesten leveres fra samme elektroniske utstyr.

18) Funksjonen til et samtrafikkpunkt på Internett (IXP) er å sammenkople nett. Et IXP gir ikke netttilgang og fungerer ikke som transittleverandør eller transittoperatør. Et IXP besørger heller ikke andre tjenester uten tilknytning til samtrafikk, men dette hindrer ikke en IXP-operatør i å yte andre tjenester. Formålet med et IXP er å sammenkople nett som er teknisk og organisatorisk atskilt. Begrepet «autonomt system» brukes til å beskrive et teknisk frittstående nett.

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

UOFFISIELL OVERSETTELSE

19) Medlemsstatene bør ha ansvar for å fastsette hvilke foretak som oppfyller kriteriene i definisjonen av yter av samfunnsviktige tjenester. For å sikre en ensartet tilnærming bør definisjonen av yter av samfunnsviktige tjenester anvendes konsekvent av alle medlemsstatene. For dette formål inneholder dette direktiv bestemmelser om vurdering av foretak som er virksomme i bestemte sektorer og delsektorer, opprettelse av en liste over samfunnsviktige tjenester, overveielse av en felles liste over forhold på tvers av sektorer for å avgjøre om en hendelse vil kunne ha en betydelig forstyrrende virkning, en samrådsprosess som involverer relevante medlemsstater når det gjelder foretak som yter tjenester i mer enn én medlemsstat, og støtte til samarbeidsgruppen i identifikasjonsprosessen. For å sikre at eventuelle endringer i markedet gjenspeiles riktig bør listen over identifiserte ytere gjennomgås jevnlig av medlemsstatene og ajourføres ved behov. Til slutt bør medlemsstatene framlegge for Kommisjonen de nødvendige opplysninger for å vurdere i hvilken grad denne felles metoden har gjort det mulig for medlemsstatene å anvende definisjonen på en ensartet måte.

20) I forbindelse med identifisering av ytere av samfunnsviktige tjenester bør medlemsstatene, minst for hver delsektor som er omhandlet i dette direktiv, vurdere hvilke tjenester som må anses som grunnleggende for å opprettholde viktig samfunnsmessig og økonomisk virksomhet, samt om foretakene som er oppført på listen over de sektorer og delsektorer som er nevnt i dette direktiv og yter disse tjenestene, oppfyller kriteriene for identifikasjon av ytere. Ved vurderingen av hvorvidt et foretak yter en tjeneste som er grunnleggende for å opprettholde viktig samfunnsmessig eller økonomisk virksomhet, er det tilstrekkelig å undersøke hvorvidt foretaket yter en tjeneste som er oppført på listen over samfunnsviktige tjenester. Videre bør det dokumenteres at ytingen av den samfunnsviktige tjenesten er avhengig av nett- og informasjonssystemer. Avslutningsvis bør medlemsstatene, når de vurderer om en hendelse vil kunne ha en betydelig forstyrrende virkning på ytingen av tjenesten, ta hensyn til en rekke forhold på tvers av sektorer samt til eventuelle sektorspesifikke forhold.

21) For å identifisere ytere av samfunnsviktige tjenester innebærer virksomhet i en medlemsstat en effektiv og faktisk utøvelse 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 av avgjørende betydning i den forbindelse.

22) Det er mulig at foretak som driver virksomhet i de sektorer og delsektorer som er nevnt i dette direktiv, yter både samfunnsviktige og ikke-samfunnsviktige tjenester. I sektoren for lufttransport yter for eksempel lufthavner tjenester som en medlemsstat kan anse som samfunnsviktige, som styring av rullebaner, men også en rekke tjenester som kan anses som ikke-samfunnsviktige, som tilrettelagte handleområder. Ytere av samfunnsviktige tjenester bør være underlagt de særlige sikkerhetskravene bare med hensyn til de tjenestene som anses som samfunnsviktige. For å identifisere ytere bør medlemsstatene derfor utarbeide en liste over tjenester som anses som samfunnsviktige.

23) Listen bør inneholde alle tjenester som ytes på territoriet til en medlemsstat som oppfyller kravene i dette direktiv. 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 typer av samfunnsviktige tjenester i en bestemt sektor som er nevnt i dette direktiv, slik at de kan holdes atskilt fra ikke-samfunnsviktige tjenester som et foretak med virksomhet i en bestemt sektor kan være ansvarlig for. Listen over tjenester som hver enkelt medlemsstat oppretter, vil kunne bidra ytterligere til vurderingen av lovgivningsmessig praksis i hver medlemsstat med sikte på å sikre en overordnet sammenheng i identifikasjonsprosessen mellom medlemsstatene.

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

25) Som følge av identifikasjonsprosessen bør medlemsstatene vedta nasjonale tiltak for å fastsette hvilke foretak som er underlagt forpliktelser med hensyn til sikkerhet i nett- og informasjonssystemer. Dette kan oppnås ved å vedta en liste over alle ytere av samfunnsviktige tjenester eller ved å vedta nasjonale tiltak, herunder objektive målbare kriterier, for eksempel yterens produksjon eller antall brukere, som gjør det mulig å bestemme hvilke foretak som er underlagt forpliktelser med hensyn til sikkerhet i nett- og informasjonssystemer. De nasjonale tiltakene, uansett om de allerede er vedtatt eller om de vedtas innenfor rammen av dette direktiv, bør omfatte alle rettslige tiltak, administrative tiltak og strategier som gjør det mulig å identifisere ytere av samfunnsviktige tjenester i henhold til dette direktiv.

UOFFISIELL OVERSETTELSE

26) For å gi en indikasjon på hvilken betydning identifiserte ytere av samfunnsviktige tjenester har i den berørte sektoren, bør medlemsstatene ta hensyn til yternes antall og størrelse, for eksempel når det gjelder markedsandeler eller mengden som er produsert eller levert, uten å være forpliktet til å gi videre opplysninger som viser hvilke ytere som er identifisert.

27) For å avgjøre om en hendelse vil kunne ha en betydelig forstyrrende virkning på en samfunnsviktig tjeneste bør medlemsstatene ta hensyn til en rekke ulike forhold, for eksempel antall brukere som er avhengige av tjenesten til private eller yrkesmessige formål. Bruken av nevnte tjeneste kan skje direkte, indirekte eller gjennom formidling. Når medlemsstatene skal vurdere i hvilken grad og hvor lenge en hendelse vil kunne påvirke økonomisk og samfunnsmessig virksomhet eller offentlig sikkerhet, bør de også vurdere hvor lang tid det sannsynligvis vil ta før avbruddet får en negativ virkning.

28) I tillegg til forhold på tvers av sektorer bør de også vurdere sektorspesifikke forhold for å avgjøre om en hendelse vil kunne ha en betydelig forstyrrende virkning på ytingen av en samfunnsviktig tjeneste. Med hensyn til energileverandører kan slike forhold for eksempel omfatte mengden eller andelen elektrisitet som er produsert nasjonalt; for oljeleverandører mengden olje per dag; for lufttransport, herunder lufthavner og luftfartsselskaper, jernbanetransport og sjøhavner, den nasjonale andelen av trafikkmengden og antall passasjerer eller størrelsen på fraktvirksomheten per år; for bankvirksomhet eller finansmarkedenes infrastrukturer deres betydning for systemet på grunnlag av samlede eiendeler eller forholdet mellom samlede eiendeler og BNP; for helsesektoren antall pasienter som tjenesteyteren pleier per år; for produksjon, behandling og forsyning av vann mengden, antall og typer brukere som forsynes, herunder for eksempel sykehus, organisasjoner i offentlig sektor eller enkeltpersoner, samt om det finnes alternative vannkilder som dekker samme geografiske område.

29) For å oppnå og opprettholde et høyt nivå av sikkerhet i nett- og informasjonssystemer bør hver medlemsstat ha en nasjonal strategi for sikkerhet i nett- og informasjonssystemer som definerer strategiske mål og konkrete politiske tiltak som skal gjennomføres.

30) På bakgrunn av forskjellene i nasjonale styringsstrukturer og for å verne 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 nett- og informasjonssystemer hos ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester i henhold til dette direktiv.

31) For å legge til rette for samarbeid og kommunikasjon over landegrensene og gjøre det mulig å gjennomføre dette direktiv effektivt må hver medlemsstat, uten at det berører sektorspesifikke regelverk, utpeke et nasjonalt felles kontaktpunkt med ansvar for å samordne spørsmål knyttet til sikkerhet i nett- og informasjonssystemer og samarbeid over landegrensene 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 direktiv. Ettersom dette direktiv har som mål å forbedre det indre markeds virkemåte ved å skape tillit og tiltro, må medlemsstatenes organer kunne samarbeide effektivt med økonomiske aktører og ha en struktur som er forenlig med dette.

32) Vedkommende myndigheter eller enheter for håndtering av digitale hendelser («CSIRT-enheter») bør motta meldinger om hendelser. De felles kontaktpunktene bør ikke motta meldinger om eventuelle 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 meldinger om hendelser 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 identiteten til ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester, ettersom opplysninger om identiteten til melderen ikke er påkrevd for utvekslingen av beste praksis i samarbeidsgruppen. Den sammenfattende rapporten bør omfatte opplysninger om antall mottatte meldinger og arten av de meldte hendelsene, for eksempel type sikkerhetsbrudd, alvorlighetsgrad eller varighet.

34) Medlemsstatene bør ha tilstrekkelige tekniske og organisatoriske ressurser til å forebygge, avdekke, håndtere og begrense virkningen av hendelser og risikoer knyttet til nett- og informasjonssystemer. 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 eventuelle 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 betydningen av internasjonalt samarbeid på

UOFFISIELL OVERSETTELSE

området datasikkerhet bør CSIRT-enheter kunne delta i internasjonale samarbeidsnett i tillegg til CSIRT-nettet som opprettes ved dette direktiv.

35) Ettersom de fleste nett- og informasjonssystemer drives privat, er samarbeidet 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 sikre sikkerheten i nett- og informasjonssystemer. Samarbeidsgruppen bør ved behov kunne innby berørte parter til drøftinger. For å oppmuntre effektivt til utveksling av opplysninger og beste praksis er det viktig å sikre at samarbeidet ikke innebærer ulemper for ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester som deltar i slik utveksling.

36) ENISA bør bistå medlemsstatene og Kommisjonen ved å gi sakkunnskap og råd og ved å fremme utveksling av beste praksis. Særlig ved anvendelsen av dette direktiv bør Kommisjonen og medlemsstatene kunne rådføre seg med ENISA. For å bygge opp kapasitet og kunnskap blant medlemsstatene bør samarbeidsgruppen også fungere som et verktøy for utveksling av beste praksis, drøftinger av medlemsstatenes ressurser og beredskap og, på frivillig grunnlag, bistå sine medlemmer med å evaluere nasjonale strategier for sikkerhet i nett- og informasjonssystemer, bygge opp kapasiteten og evaluere øvelser knyttet til sikkerheten i nett- og informasjonssystemer.

37) Når det er hensiktsmessig, bør medlemsstatene kunne anvende eller tilpasse eksisterende organisasjonsstrukturer eller strategier ved anvendelsen av dette direktiv.

38) De respektive oppgavene til samarbeidsgruppen og ENISA er innbyrdes avhengige og utfyller hverandre. Generelt bør ENISA bistå samarbeidsgruppen med utførelsen av dens oppgaver i samsvar med ENISAs mål som fastsatt i 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 nett- og informasjonssystemer i henhold til gjeldende og framtidige unionsrettsakter. ENISA bør særlig yte bistand på de områder som svarer til ENISAs egne oppgaver som fastsatt i forordning (EU) nr. 526/2013, som er å analysere strategier for sikkerhet i nett- og informasjonssystemer, støtte organiseringen og gjennomføringen av øvelser på unionsplan som gjelder sikkerhet i nett- og informasjonssystemer, samt utveksle opplysninger og beste praksis med hensyn til holdningsskapende tiltak og opplæring. ENISA bør også delta i utarbeidingen av retningslinjer for sektorspesifikke kriterier som skal brukes til å fastsette betydningen til virkningen av en hendelse.

39) For å fremme avansert sikkerhet for nett- 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 nett- og informasjonssystemer som kan påvirke deres arbeid, idet det tas hensyn til eksisterende ordninger for utveksling av opplysninger som omfattes av restriksjoner. Når samarbeidsgruppen samarbeider med myndigheter som har ansvar for håndheving av loven, om sikkerhetsaspekter ved nett- og informasjonssystemer som kan påvirke deres arbeid, bør samarbeidsgruppen respektere eksisterende informasjonskanaler og etablerte nett.

40) Opplysninger om hendelser blir stadig mer verdifulle for allmennheten og foretak, særlig små og mellomstore bedrifter. I noen tilfeller er allerede disse opplysningene tilgjengelige via nettsteder på nasjonalt plan, på språket i en bestemt stat, og først og fremst om hendelser og tilfeller med en nasjonal dimensjon. Ettersom foretak i stadig større grad driver virksomhet på tvers av landegrensene og borgere bruker nettbaserte tjenester, bør opplysninger om hendelser finnes i aggregert form på unionsplan. CSIRT-nettets sekretariat oppfordres til å opprette et nettsted eller ha en særskilt side på et eksisterende nettsted der generelle opplysninger om større hendelser som har funnet sted i hele Unionen, gjøres tilgjengelig for allmennheten med særlig fokus på foretakenes interesser og behov. CSIRT-enheter som deltar i CSIRT-nettet, oppfordres til frivillig å oppgi opplysningene som skal offentliggjøres på nettstedet, uten at de omfatter fortrolige eller følsomme opplysninger.

41) Dersom opplysninger anses som fortrolige i samsvar med Unionens og nasjonale regler for forretningshemmeligheter, bør denne fortroligheten ivaretas ved gjennomføring av virksomhet og oppfyllelse av mål i henhold til dette direktiv.

42) Øvelser som simulerer hendelsesscenarioer i sanntid, er avgjørende for å teste medlemsstatenes beredskap og samarbeid når det

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

UOFFISIELL OVERSETTELSE

gjelder sikkerhet i nett- og informasjonssystemer. Øvelsesserien CyberEurope, som ENISA samordner med deltakelse fra medlemsstatene, er et nyttig verktøy for å teste og utarbeide anbefalinger om hvordan håndtering av hendelser på unionsplan bør forbedres over tid. Ettersom medlemsstatene for øyeblikket ikke er forpliktet til verken å planlegge eller delta i øvelser, bør opprettelsen av CSIRT-nettet i henhold til dette direktiv gi medlemsstatene mulighet til å delta i øvelser på grunnlag av nøyaktig planlegging og strategiske valg. Samarbeidsgruppen som opprettes i henhold til dette direktiv, bør drøfte de strategiske beslutningene om øvelser, særlig, men ikke utelukkende med hensyn til 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-nettet med sakkunnskap og råd.

43) Tatt i betraktning at sikkerhetsproblemene som påvirker nett- og informasjonssystemer, har en global dimensjon, er det behov for tettere internasjonalt samarbeid for å forbedre sikkerhetsstandarder og utveksling av opplysninger, og for å fremme en felles global tilnærming til sikkerhetsspørsmål.

44) Ansvaret for å sikre sikkerheten i nett- og informasjonssystemer ligger i stor grad 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 like vilkår er også avgjørende for at samarbeidsgruppen og CSIRT-nettet skal fungere effektivt, for å sikre effektivt samarbeid fra alle medlemsstater.

45) Dette direktiv får anvendelse bare på offentlige forvaltninger som er identifisert som ytere av samfunnsviktige tjenester. Det er derfor medlemsstatenes ansvar å sikre sikkerheten i nett- og informasjonssystemer hos offentlige forvaltninger som ikke omfattes av dette direktivs virkeområde.

46) Risikohåndteringstiltak omfatter tiltak for å identifisere eventuelle risikoer for hendelser med sikte på å forebygge, avdekke og håndtere hendelser og begrense deres virkninger. Sikkerheten i nett- og informasjonssystemer omfatter sikkerheten til lagrede, overførte og behandlede data.

47) Vedkommende myndigheter bør fortsatt ha mulighet til å vedta nasjonale retningslinjer om hvilke omstendigheter som forplikter ytere av samfunnsviktige tjenester til å melde hendelser.

48) Mange foretak i Unionen er avhengige av tilbydere av digitale tjenester for å levere tjenestene sine. Ettersom visse digitale tjenester kan være en viktig ressurs for brukerne, herunder ytere av samfunnsviktige tjenester, og disse brukerne ikke alltid har tilgjengelige alternativer, bør dette direktiv også få anvendelse på tilbydere av slike tjenester. Sikkerheten, kontinuiteten og påliteligheten til den typen digitale tjenester som er nevnt i dette direktiv, er for mange foretak avgjørende for å 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 avgjørende for at foretak som er avhengige av dem, skal fungere godt, og særlig for disse foretakenes deltakelse i det indre marked og handel over landegrensene i hele Unionen. Tilbydere av digitale tjenester som omfattes av dette direktiv, er de tilbydere som anses å tilby digitale tjenester som mange foretak i Unionen i økende grad er avhengige av.

49) Tilbydere av digitale tjenester bør sikre et sikkerhetsnivå som står i forhold til graden av risiko forbundet med de digitale tjenestene de leverer, tatt i betraktning tjenestenes betydning for andre foretaks virksomhet i Unionen. Graden av risiko for ytere av samfunnsviktige tjenester, som ofte er avgjørende for å opprettholde viktig samfunnsmessig og økonomisk virksomhet, er i praksis 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 som de anser som hensiktsmessige for å håndtere risikoene knyttet til sikkerheten i sine nett- og informasjonssystemer. Tilbydere av digitale tjenester bør på grunn av sin tverrnasjonale karakter være underlagt en mer harmonisert tilnærming på unionsplan. Fastsettelsen og gjennomføringen av slike tiltak bør fremmes ved gjennomføringsrettsakter.

50) Selv om maskinvareprodusenter og programvareutviklere verken er ytere av samfunnsviktige tjenester eller tilbydere av digitale tjenester, øker produktene deres sikkerheten i nett- og informasjonssystemer. De spiller derfor en viktig rolle med hensyn til å gjøre ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester i stand til å sikre sine nett- og informasjonssystemer.

UOFFISIELL OVERSETTELSE

Slike maskinvare- og programvareprodukter omfattes allerede av gjeldende 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 sikre sikkerheten i nett- og informasjonssystemene som de bruker. Dette er først og fremst private nett- og informasjonssystemer som ivaretas av internt IT-personell eller der sikkerhetsoppgavene er satt ut. Sikkerhets- og meldingskravene bør få anvendelse på berørte ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester, uansett om de utfører vedlikehold av nett- og informasjonssystemene sine internt eller setter det ut.

53) For å unngå en uforholdsmessig stor økonomisk og administrativ byrde for ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester bør kravene stå i forhold til risikoen som det berørte nett- og informasjonssystemet utgjør, idet det tas hensyn til nåværende utviklingstrinn i teknikken for slike tiltak. Når det gjelder tilbydere av digitale tjenester bør disse kravene ikke få anvendelse på svært små og små bedrifter.

54) Når offentlige forvaltninger i medlemsstatene bruker tjenester som tilbys av tilbydere av digitale tjenester, særlig skytjenester, vil de kanskje kreve at tilbydere av slike tjenester sørger for ytterligere sikkerhetstiltak utover de som tilbydere av digitale tjenester normalt ville tilby i samsvar med kravene i dette direktiv. De bør kunne gjøre dette ved hjelp av avtaleforpliktelser.

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

56) Dette direktiv bør ikke hindre medlemsstatene i å vedta nasjonale tiltak som krever at offentlige organer fastsetter særskilte sikkerhetskrav når de inngår avtaler om skytjenester. Slike nasjonale tiltak bør få anvendelse på det berørte offentlige organet og ikke på tilbyderen av skytjenester.

57) Tatt i betraktning de grunnleggende forskjellene mellom ytere av samfunnsviktige tjenester, særlig deres direkte forbindelse med fysisk infrastruktur, og tilbydere av digitale tjenester, særlig deres grensekryssende karakter, bør dette direktiv differensieres med hensyn til harmonisering når det gjelder disse to gruppene av foretak. For ytere av samfunnsviktige tjenester bør medlemsstatene kunne identifisere de relevante aktørene og innføre strengere krav enn dem som er fastsatt i dette direktiv. Medlemsstatene bør ikke identifisere tilbydere av digitale tjenester, ettersom dette direktiv bør få anvendelse på alle tilbydere av digitale tjenester som omfattes av dette direktivs virkeområde. I tillegg bør dette direktiv og gjennomføringsrettsaktene som vedtas i henhold til det, sikre et høyt nivå av harmonisering for tilbydere av digitale tjenester med hensyn til sikkerhets- og meldingskrav. Dette bør gjøre det mulig å behandle tilbydere av digitale tjenester på en ensartet måte i hele Unionen, på en måte som står i forhold til deres karakter og graden av risiko de kan stå overfor.

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

59) Vedkommende myndigheter bør ta behørig hensyn til nødvendigheten av å bevare uformelle og pålitelige kanaler for utveksling av opplysninger. 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 ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester som rapporterer hendelser. Ved gjennomføringen av meldingsplikten bør vedkommende myndigheter og CSIRT-enhetene rette særlig oppmerksomhet mot behovet for å holde opplysninger om produkters sårbarhet strengt fortrolige inntil det sendes ut egnede sikkerhetsoppdateringer.

60) Tilbydere av digitale tjenester bør omfattes av et mindre omfattende og reaktivt tilsyn i ettertid som er tilpasset deres type tjenester

UOFFISIELL OVERSETTELSE

og virksomhet. Den berørte vedkommende myndighet bør derfor bare treffe tiltak når den har mottatt dokumentasjon, for eksempel fra tilbyderen av digitale tjenester selv, fra en annen vedkommende myndighet, herunder en vedkommende myndighet i en annen medlemsstat, eller av en bruker av tjenesten, på at en tilbyder av digitale tjenester ikke oppfyller kravene i dette direktiv, særlig etter en hendelse. Den vedkommende myndigheten bør derfor ikke ha en generell plikt til å føre tilsyn med tilbydere av digitale tjenester.

61) Vedkommende myndigheter bør ha de nødvendige midler til å utføre sine oppgaver, herunder myndighet til å innhente tilstrekkelige opplysninger for å vurdere graden av sikkerhet i nett- og informasjonssystemer.

62) Hendelser kan oppstå som følge av kriminell virksomhet, og forebygging, etterforskning og rettsforfølging av dette støttes av samordning og samarbeid mellom ytere av samfunnsviktige tjenester, tilbydere av digitale tjenester, vedkommende myndigheter og myndigheter med ansvar for håndheving av loven. Dersom det er mistanke om at en hendelse er knyttet til alvorlig kriminell virksomhet i henhold til unionsretten eller nasjonal lovgivning, bør medlemsstatene oppmuntre ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester til å rapportere hendelser av antatt alvorlig strafferettslig art til de relevante myndigheter med ansvar for håndheving av loven. Dersom det er relevant, er det ønskelig at samordningen mellom forskjellige medlemsstaters vedkommende myndigheter og myndigheter med ansvar for håndheving av loven gjøres lettere av Det europeiske senter for bekjempelse av datakriminalitet (EC3) og ENISA.

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

64) Jurisdiksjon med hensyn til tilbydere av digital tjenester bør tilskrives den medlemsstaten der den berørte tilbyderen av digitale tjenester har sitt hovedforetak i Unionen, som i prinsippet svarer til det sted der tilbyderen har sitt hovedkontor i Unionen. En virksomhet innebærer en effektiv og faktisk utøvelse 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 av avgjørende betydning i den forbindelse. Dette kriteriet bør ikke være avhengig av om nett- og informasjonssystemer fysisk befinner seg på et bestemt sted; forekomst og bruk av slike systemer utgjør ikke i seg selv et slikt hovedforetak og er derfor ikke kriterier for å fastsette hovedforetaket.

65) En tilbyder av digital tjenester som ikke er etablert i Unionen, og som tilbyr tjenester i Unionen, bør 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 planlegger å tilby tjenester til personer i én eller flere medlemsstater. Det forhold alene at et nettsted tilhørende tilbyderen av digitale tjenester eller en formidler, eller en e-postadresse og andre kontaktopplysninger, er tilgjengelige i Unionen, eller at det brukes et språk som vanligvis brukes i tredjestaten der tilbyderen av digitale tjenester er etablert, er ikke tilstrekkelig til å fastslå en slik hensikt. Imidlertid kan forhold som for eksempel bruk av et språk eller en valuta som vanligvis brukes i én eller flere medlemsstater med mulighet til å bestille tjenester på det aktuelle språket, eller omtale av kunder eller brukere i Unionen, gjøre det klart at tilbyderen av digitale tjenester planlegger 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 direktiv, herunder rapportering av hendelser.

66) Standardisering av sikkerhetskrav er en markedsdrevet prosess. For å sikre en ensartet anvendelse av sikkerhetsstandarder bør medlemsstatene oppmuntre til overholdelse av eller samsvar med angitte standarder for å sikre et høyt nivå av sikkerhet i nett- 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]).

([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).

UOFFISIELL OVERSETTELSE

67) Foretak som faller utenfor dette direktivs virkeområde, kan oppleve hendelser som virker betydelig inn på de tjenestene de tilbyr. Dersom disse foretakene mener det er i offentlighetens interesse å melde forekomsten av slike hendelser, bør de kunne gjøre dette på frivillig grunnlag. Disse meldingene bør behandles av vedkommende myndighet eller CSIRT-enheten når slik behandling ikke utgjør en uforholdsmessig stor eller urimelig byrde for de berørte medlemsstatene.

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

69) Når den vedtar gjennomføringsrettsakter om sikkerhetskravene til tilbydere av digitale tjenester, bør Kommisjonen 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 utstyr: fysisk sikkerhet og miljøsikkerhet, forsyningssikkerhet, kontroll av tilgang til nett- og informasjonssystemer og integriteten til nett- og informasjonssystemer; når det gjelder håndtering av hendelser: prosedyrer for hendelseshåndtering, kapasitet til å påvise hendelser, hendelsesrapportering og kommunikasjon; når det gjelder håndtering av kontinuitet i virksomheten: 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 nett- og informasjonstjenester, sikkerhetsvurderinger og overvåking av samsvar.

70) Ved gjennomføringen av dette direktiv bør Kommisjonen samarbeide etter behov med relevante sektorkomiteer og relevante organer som er opprettet på unionsplan på de områdene som omfattes av dette direktiv.

71) Kommisjonen bør med jevne mellomrom ta dette direktiv opp til ny vurdering i samråd med berørte parter, særlig for å bestemme om det er nødvendig å endre det for å ta hensyn til samfunnsutviklingen, den politiske utvikling, den teknologiske utviklingen eller markedssituasjonen.

72) Utveksling av opplysninger om risikoer og hendelser innenfor samarbeidsgruppen og nettet av CSIRT-enheter og overholdelse av kravet om å melde hendelser til vedkommende nasjonale myndigheter eller CSIRT-enhetene, kan kreve behandling av personopplysninger. En slik behandling bør være i samsvar med europaparlaments- og rådsdirektiv 95/46/EF([10]) og europaparlaments- og rådsforordning (EF) nr. 45/2001([11]). Ved anvendelsen av dette direktiv bør europaparlaments- og rådsforordning (EF) nr. 1049/2001([12]) få anvendelse i nødvendig omfang.

73) EUs datatilsyn er blitt 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 direktiv, som er å oppnå et høyt felles nivå for sikkerhet i nett- og informasjonssystemer i hele Unionen, ikke kan nås i tilstrekkelig grad av medlemsstatene og derfor på grunn av tiltakets virkninger bedre kan nås på unionsplan, kan Unionen treffe tiltak i samsvar med nærhetsprinsippet som fastsatt i traktatens artikkel 5. I samsvar med forholdsmessighetsprinsippet fastsatt i nevnte artikkel, går dette direktiv ikke lenger enn det som er nødvendig for å nå dette målet.

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

UOFFISIELL OVERSETTELSE

([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).

([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.

VEDTATT DETTE DIREKTIV:

KAPITTEL I

ALMINNELIGE BESTEMMELSER

Artikkel 1

Formål og virkeområde

1. I dette direktiv fastsettes tiltak med sikte på å oppnå et høyt felles nivå for sikkerhet i nett- og informasjonssystemer i Unionen for å forbedre virkemåten til det indre marked.

2. I den forbindelse blir det i dette direktiv

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

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

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

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

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

3. Sikkerhets- og meldingskravene fastsatt i dette direktiv 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 direktiv 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 for forretningshemmeligheter, utveksles med Kommisjonen og andre relevante myndigheter bare dersom utvekslingen er nødvendig for anvendelsen av dette direktiv. Utvekslingen skal begrense seg til opplysninger som er relevante og står i forhold til formålet. Slik utveksling av opplysninger skal sikre at opplysningene behandles fortrolig og beskytte sikkerhets- og forretningsinteressene til ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester.

6. Dette direktiv 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 medlemsstatene anser å stride mot deres vesentlige sikkerhetsinteresser, og for å opprettholde lov og orden, særlig for å muliggjøre etterforskning, avsløring og rettslig forfølging av straffbare handlinger.

7. Dersom en sektorspesifikk unionsrettsakt krever at ytere av samfunnsviktige tjenester eller tilbydere av digitale tjenester enten skal sikre sikkerheten i sine nett- og informasjonssystemer eller melde hendelser, forutsatt at slike krav i praksis minst tilsvarer

([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).

UOFFISIELL OVERSETTELSE

forpliktelsene fastsatt i dette direktiv, skal bestemmelsene i den sektorspesifikke unionsrettsakten få anvendelse.

Artikkel 2

Behandling av personopplysninger

1. Personopplysninger som behandles i henhold til dette direktiv, skal behandles i samsvar med direktiv 95/46/EF.

2. Personopplysninger som behandles av Unionens institusjoner og organer i henhold til dette direktiv, skal behandles i samsvar med forordning (EF) nr. 45/2001.

Artikkel 3

Minsteharmonisering

Uten at det berører artikkel 16 nr. 10 og deres forpliktelser i henhold til unionsretten kan medlemsstatene vedta eller opprettholde bestemmelser med sikte på å oppnå et høyere nivå for sikkerhet i nett- og informasjonssystemer.

Artikkel 4

Definisjoner

I dette direktiv menes med:

1) «nett- og informasjonssystem»

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

   b) en innretning eller gruppe av innbyrdes forbundne eller tilknyttede innretninger, hvorav én eller flere av dem ved hjelp av et program utfører automatisk behandling av digitale data, eller

   c) digitale data som lagres, behandles, innhentes eller overføres med elementene som omfattes av bokstav a) og b) i forbindelse med drift, bruk, vern og vedlikehold,

2) «sikkerhet i nett- og informasjonsystemer» den evnen nett eller informasjonssystemer har til å tåle, på et gitt tillitsnivå, enhver handling som går ut over tilgjengeligheten, autentisiteten, integriteten eller tilliten til lagrede eller overførte eller behandlede data eller tilknyttede tjenester som tilbys eller er tilgjengelige via slike nett- og informasjonssystemer,

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

4) «yter av samfunnsviktige tjenester» et offentlig eller privat foretak av en type som er nevnt i vedlegg II, og 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]) og av en type oppført i vedlegg III,

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

7) «hendelse» enhver hendelse som har en reell negativ virkning på sikkerheten i nett- og informasjonssystemer,

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

([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).

UOFFISIELL OVERSETTELSE

9) «risiko» enhver rimelig identifiserbar omstendighet eller hendelse med en mulig negativ virkning på sikkerheten i nett- 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, som vedkommende nasjonale myndighet eller en CSIRT-enhet eventuelt kan henvende seg til i stedet for tilbyderen av digitale tjenester med hensyn til forpliktelsene som tilbyderen av digitale tjenester har i henhold til dette direktiv,

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 nettstruktur som muliggjør sammenkopling av mer enn to uavhengige og selvstendige systemer, først og fremst for å legge til rette for samtrafikk på Internett; et IXP sørger for sammenkopling bare for selvstendige systemer; et IXP krever ikke at internettrafikk som passerer mellom to deltakende selvstendige systemer, passerer gjennom et tredje selvstendig system, og det verken endrer eller griper forstyrrende inn i slik trafikk,

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

15) «tilbyder av DNS-tjenester» et foretak som leverer DNS-tjenester på Internett,

16) «registerenhet for toppdomener» et foretak som forvalter og driver registrering av domenenavn på Internett 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 brukere å foreta søk på i prinsippet alle nettsteder eller nettsteder på et bestemt språk, på grunnlag av en forespørsel om et hvilket som helst emne i form av et nøkkelord, en setning eller andre inndata, og som viser lenker hvor det er mulig å finne informasjon om det forespurte innholdet,

19) «skytjeneste» en digital tjeneste som gir tilgang til en skalerbar og fleksibel 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 ytere av samfunnsviktige tjenester som er etablert på deres territorium.

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

a) Et foretak yter en tjeneste som er grunnleggende for å opprettholde viktig samfunnsmessig og/eller økonomisk virksomhet.

b) Ytingen av tjenesten avhenger av nett- og informasjonssystemer.

c) En hendelse vil få en betydelig forstyrrende virkning på ytingen 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 et foretak yter en tjeneste nevnt i nr. 2 bokstav a) i to eller flere medlemsstater, skal disse medlemsstatene delta i samråd med hverandre. Samrådet skal finne sted før det tas en beslutning om identifikasjon.

5. Medlemsstatene skal regelmessig og minst hvert annet år etter 9. mai 2018 gjennomgå og eventuelt ajourføre listen over

([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).

UOFFISIELL OVERSETTELSE

identifiserte ytere av samfunnsviktige tjenester.

6. Rollen til samarbeidsgruppen skal i samsvar med oppgavene nevnt i artikkel 11 være å hjelpe medlemsstatene med å være konsekvente i arbeidet med å identifisere ytere av samfunnsviktige tjenester.

7. Med henblikk på gjennomgåelsen nevnt i artikkel 23 skal medlemsstatene innen 9. november 2018 og deretter hvert annet år framlegge for Kommisjonen de opplysninger som er nødvendige for å vurdere gjennomføringen av dette direktiv, særlig ensartetheten i medlemsstatenes metoder for å identifisere ytere av samfunnsviktige tjenester. Opplysningene skal minst omfatte følgende:

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

b) listen over tjenester nevnt i nr. 3,

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

d) terskelverdier, dersom slike finnes, for å bestemme det relevante forsyningsnivået i forhold til antall brukere som er avhengig av tjenesten som nevnt i artikkel 6 nr. 1 bokstav a), eller i forhold til betydningen av denne yteren av samfunnsviktige tjenester som nevnt i artikkel 6 nr. 1 bokstav f).

For å bidra til at det foreligger sammenlignbare opplysninger, kan Kommisjonen, idet det tas størst mulig hensyn til uttalelsen fra ENISA, vedta egnede tekniske retningslinjer for parametrene for de opplysninger som er nevnt i dette nummer.

Artikkel 6

Betydelig forstyrrende virkning

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

a) antall brukere som er avhengige av tjenesten som ytes av det berørte foretaket,

b) avhengigheten til andre sektorer nevnt i vedlegg II av tjenesten som ytes av foretaket,

c) virkningen som hendelser vil kunne ha med hensyn til omfang og varighet på økonomisk og samfunnsmessig virksomhet eller offentlig sikkerhet,

d) foretakets markedsandel,

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

f) foretakets betydning for å opprettholde et tilstrekkelig tjenestenivå, idet det tas hensyn til tilgjengeligheten av alternative metoder for å yte tjenesten.

2. For å avgjøre om en hendelse vil kunne ha en betydelig forstyrrende virkning skal medlemsstatene også, når det er hensiktsmessig, ta hensyn til sektorspesifikke forhold.

UOFFISIELL OVERSETTELSE

KAPITTEL II

NASJONALE RAMMER FOR SIKKERHET I NETT- OG INFORMASJONSSYSTEMER

Artikkel 7

Nasjonal strategi for sikkerhet i nett- og informasjonssystemer

1. Hver medlemsstat skal vedta en nasjonal strategi for sikkerhet i nett- og informasjonssystemer som definerer strategiske mål og en egnet politikk og egnede lovgivningsmessige tiltak med henblikk på å oppnå og opprettholde et høyt nivå av sikkerhet i nett- og informasjonssystemer, og som minst omfatter sektorene nevnt i vedlegg II og tjenestene nevnt i vedlegg III. Den nasjonale strategien for sikkerhet i nett- og informasjonssystemer skal særlig omhandle følgende:

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

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

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

d) en angivelse av utdanningsprogrammer, holdningsskapende tiltak og opplæringsprogrammer forbundet med den nasjonale strategien for sikkerhet i nett- og informasjonssystemer,

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

f) en risikovurderingsplan for å identifisere eventuelle risikoer,

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

2. Medlemsstatene kan be om bistand fra ENISA for å utvikle nasjonale strategier for sikkerhet i nett- og informasjonssystemer.

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

Artikkel 8

Vedkommende nasjonale myndigheter og et felles kontaktpunkt

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

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

3. Hver medlemsstat skal utpeke et nasjonalt felles kontaktpunkt for sikkerhet i nett- og informasjonssystemer («felles kontaktpunkt»). Medlemsstatene kan overlate 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 samarbeidet over landegrensene mellom medlemsstatenes myndigheter og relevante myndigheter i andre medlemsstater og med samarbeidsgruppen nevnt i artikkel 11 og CSIRT-nettet

UOFFISIELL OVERSETTELSE

omhandlet i artikkel 12.

5. Medlemsstatene skal sikre at vedkommende myndigheter og de felles kontaktpunktene har tilstrekkelige ressurser til å kunne utføre effektivt og formålstjenlig oppgavene de blir pålagt og dermed nå målene i dette direktiv. 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 lovgivning, rådføre seg og samarbeide med den relevante nasjonale myndighet med ansvar for håndheving av loven og med nasjonale personvernmyndigheter.

7. Hver medlemsstat skal uten opphold underrette Kommisjonen om utpekingen av vedkommende myndighet og det felles kontaktpunktet, deres oppgaver og eventuelle senere endringer 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 nr. 1 i vedlegg I, som minst omfatter 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-enheter har tilstrekkelige ressurser til å kunne utføre sine oppgaver effektivt som fastsatt i nr. 2 i vedlegg I.

Medlemsstatene skal sikre et effektivt, formålstjenlig og sikkert samarbeid mellom deres CSIRT-enheter og CSIRT-nettet 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 med hensyn til oppfyllelsen av forpliktelsene fastsatt i dette direktiv.

2. Medlemsstatene skal sikre at enten vedkommende myndigheter eller CSIRT-enhetene mottar meldinger om hendelser som inngis i henhold til dette direktiv. 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 opplysninger om hendelser som meldes av ytere av samfunnsviktige tjenester i henhold til artikkel 14 nr. 3 og 5, eller av tilbydere av digitale tjenester i henhold til artikkel 16 nr. 3 og 6.

3. Medlemsstatene skal sikre at vedkommende myndigheter eller CSIRT-enhetene underretter de felles kontaktpunktene om meldinger om hendelser som inngis i henhold til dette direktiv.

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 meldte hendelser, og de tiltak som er truffet i samsvar med artikkel 14 nr. 3 og 5 og artikkel 16 nr. 3 og 6.

UOFFISIELL OVERSETTELSE

KAPITTEL III

SAMARBEID

Artikkel 11

Samarbeidsgruppe

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

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

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

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

Kommisjonen skal ivareta sekretariatet.

3. Samarbeidsgruppen skal ha følgende oppgaver:

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

b) utveksle beste praksis for utveksling av opplysninger om 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 sikre sikkerheten i nett- og informasjonssystemer,

d) drøfte ressurser og beredskap i medlemsstatene og, på frivillig grunnlag, evaluere nasjonale strategier for sikkerhet i nett- og informasjonssystemer og effektiviteten til CSIRT-enheter, samt identifisere beste praksis,

e) utveksle opplysninger og beste praksis med hensyn til holdningsskapende tiltak og opplæring,

f) utveksle opplysninger og beste praksis med hensyn til forskning og utvikling knyttet til sikkerhet i nett- og informasjonssystemer,

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

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

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 annet ledd,

k) drøfte arbeidet som er gjort med hensyn til øvelser i forbindelse med sikkerhet i nett- og informasjonssystemer, utdanningsprogrammer og opplæring, herunder arbeid utført av ENISA,

l) med ENISAs bistand utveksle beste praksis med hensyn til medlemsstatenes identifikasjon av ytere av samfunnsviktige tjenester, herunder i forbindelse med gjensidig avhengighet over landegrensene, vedrørende risikoer og hendelser,

m) drøfte metoder for rapportering av meldte hendelser som nevnt i artikkel 14 og 16.

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

UOFFISIELL OVERSETTELSE

4. Med henblikk på gjennomgåelsen nevnt i artikkel 23 skal samarbeidsgruppen innen 9. august 2018, og deretter hvert halvannet år, utarbeide en rapport om de erfaringer som er gjort med det strategiske samarbeidet i henhold til denne artikkel.

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

I henhold til første ledd skal Kommisjonen oversende det første utkastet til gjennomføringsrettsakt for komiteen nevnt i artikkel 22 nr. 1 innen 9. februar 2017.

Artikkel 12

CSIRT-nett

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

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

3. CSIRT-nettet skal ha følgende oppgaver:

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

b) på anmodning fra en CSIRT-representant fra en medlemsstat som kan bli berørt av en hendelse, utveksle og drøfte saker som berører ikke-kommersielt følsomme opplysninger knyttet til hendelsen og tilknyttede risikoer; en CSIRT-enhet fra en medlemsstat kan imidlertid nekte å bidra til diskusjonen dersom det er fare for at det kan påvirke undersøkelsen av hendelsen negativt,

c) utveksle og gjøre tilgjengelig ikke-fortrolige opplysninger om enkeltstående hendelser på frivillig grunnlag,

d) på anmodning fra en representant for en medlemsstats CSIRT-enhet, drøfte og, om mulig, finne en samordnet innsats for en hendelse som er blitt avdekket i medlemsstatens jurisdiksjon,

e) gi medlemsstatene støtte til å løse 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 øvelsene vedrørende sikkerhet i nett- og informasjonssystemer, herunder dem som organiseres av ENISA,

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

j) utarbeide retningslinjer for å lette sammenfallet mellom driftspraksiser med hensyn til anvendelsen av bestemmelsene om driftsmessig samarbeid i denne artikkel.

4. Med henblikk på gjennomgåelsen nevnt i artikkel 23 skal CSIRT-nettet innen 9. august 2018, og deretter hvert halvannet år, utarbeide en rapport om de erfaringer som er gjort med det driftsmessige samarbeidet, herunder konklusjoner og anbefalinger, i henhold til denne artikkel. Denne rapporten skal også oversendes til samarbeidsgruppen.

5. CSIRT-nettet skal fastsette sin egen forretningsorden.

UOFFISIELL OVERSETTELSE

Artikkel 13

Internasjonalt samarbeid

Unionen kan i samsvar med artikkel 218 i TEUV inngå internasjonale avtaler med tredjestater eller internasjonale organisasjoner og dermed muliggjøre og tilrettelegge for å delta 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 NETT- OG INFORMASJONSSYSTEMER SOM BRUKES AV YTERE AV SAMFUNNSVIKTIGE TJENESTER

Artikkel 14

Sikkerhetskrav og melding om hendelser

1. Medlemsstatene skal sikre at ytere av samfunnsviktige tjenester treffer hensiktsmessige og rimelige tekniske og organisatoriske tiltak for å håndtere risikoene knyttet til sikkerheten i nett- og informasjonssystemer som de bruker i sin virksomhet. Under henvisning til nåværende utviklingstrinn i teknikken skal disse tiltakene sikre et nivå for sikkerhet i nett- 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 virkningen av hendelser som påvirker sikkerheten i nett- 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 underretter vedkommende myndighet eller CSIRT-enheten om hendelser som virker betydelig inn på kontinuiteten i de samfunnsviktige tjenestene de yter. Meldinger skal inneholde opplysninger som gjør det mulig for vedkommende myndighet eller CSIRT-enheten å fastslå om hendelsen har virkninger over landegrensene. Meldingen skal ikke innebære økt ansvar for melderen.

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

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

b) hendelsens varighet,

c) størrelsen på det geografiske området som berøres 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 virker betydelig inn på kontinuiteten i samfunnsviktige tjenester i nevnte medlemsstat. I den forbindelse skal vedkommende myndighet eller CSIRT-enheten, i samsvar med unionsretten eller nasjonal lovgivning som er i samsvar med unionsretten, ivareta sikkerhets- og forretningsinteressene til yteren av samfunnsviktige tjenester, samt sikre at opplysningene i meldingen behandles fortrolig.

Når omstendighetene tillater det, skal vedkommende myndighet eller CSIRT-enheten gi yteren av samfunnsviktige tjenester som innga meldingen, relevante opplysninger om oppfølgingen av meldingen, f.eks. 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 rådspurt yteren av samfunnsviktige tjenester som innga meldingen, kan vedkommende myndighet eller CSIRT-enheten informere offentligheten om konkrete hendelser dersom offentlighetens kjennskap til disse er nødvendig for å forebygge en hendelse eller håndtere en hendelse som pågår.

7. Vedkommende myndigheter som opptrer 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

UOFFISIELL OVERSETTELSE

av virkningen av en hendelse som nevnt i nr. 4.

Artikkel 15

Gjennomføring og håndheving

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

2. Medlemsstatene skal sikre at vedkommende myndigheter har fullmakter og virkemidler til å kreve at ytere av samfunnsviktige tjenester sørger for

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

b) dokumentasjon 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 og den underliggende dokumentasjonen til rådighet for vedkommende myndighet.

Når det anmodes om slike opplysninger eller dokumentasjon, skal vedkommende myndighet angi formålet med anmodningen og presisere hvilke opplysninger som kreves.

3. På grunnlag av vurderingen av opplysninger eller resultater av sikkerhetsrevisjoner nevnt i nr. 2, kan vedkommende myndighet gi bindende instrukser til ytere av samfunnsviktige tjenester om å utbedre de påviste manglene.

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

KAPITTEL V

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

Artikkel 16

Sikkerhetskrav og melding om hendelser

1. Medlemsstatene skal sikre at tilbydere av digitale tjenester identifiserer og treffer hensiktsmessige og rimelige tekniske og organisatoriske tiltak for å håndtere risikoene knyttet til sikkerheten i nett- og informasjonssystemer som de bruker når de leverer tjenester nevnt i vedlegg III, i Unionen. Under henvisning til nåværende utviklingstrinn i teknikken skal disse tiltakene sikre et nivå for sikkerhet i nett- og informasjonssystemer som står i forhold til risikoen, idet det tas hensyn til følgende elementer:

a) sikkerheten i systemer og utstyr,

b) hendelseshåndtering,

c) håndtering av kontinuitet i virksomheten,

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 virkningen av hendelser som påvirker sikkerheten i deres nett- og informasjonssystemer, på tjenestene nevnt i vedlegg III og som tilbys i Unionen, med sikte på å sikre kontinuiteten i disse tjenestene.

UOFFISIELL OVERSETTELSE

3. Medlemsstatene skal sikre at tilbydere av digitale tjenester uten unødig opphold gir vedkommende myndighet eller CSIRT-enheten melding om enhver hendelse som virker betydelig inn på leveringen av en tjeneste som nevnt i vedlegg III og som de tilbyr i Unionen. Meldinger skal inneholde opplysninger som gjør det mulig for vedkommende myndighet eller CSIRT-enheten å fastslå omfanget av eventuelle virkninger over landegrensene. Meldingen skal ikke innebære økt ansvar for melderen.

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

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

b) hendelsens varighet,

c) størrelsen på det geografiske området som berøres av hendelsen,

d) omfanget av driftsforstyrrelser i tjenesten,

e) omfanget av virkningen på økonomisk og samfunnsmessig virksomhet.

Plikten til å melde en hendelse skal få anvendelse bare dersom tilbyderen av digitale tjenester har tilgang til opplysningene som trengs for å vurdere virkningen av en hendelse opp mot parametrene nevnt i første ledd.

5. Dersom en yter av samfunnsviktige tjenester er avhengig av en tredjemannstilbyder av digitale tjenester for å yte en tjeneste som er grunnleggende for å opprettholde viktig samfunnsmessig og økonomisk virksomhet, skal yteren av samfunnsviktige tjenester melde enhver betydelig virkning 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-enheten og felles kontaktpunkter, i samsvar med unionsretten eller nasjonal lovgivning som er i samsvar med unionsretten, ivareta sikkerhets- og forretningsinteressene til tilbyderen av digitale tjenester, samt sikre at opplysningene behandles fortrolig.

7. Etter å ha rådspurt den berørte tilbyderen av digitale tjenester, kan vedkommende myndighet eller CSIRT-enheten og, eventuelt, myndighetene eller CSIRT-enhetene i andre berørte medlemsstater, informere offentligheten om konkrete hendelser eller kreve at tilbyderen av digitale tjenester gjør det, dersom offentlighetens kjennskap til disse er nødvendig for å forebygge en hendelse eller håndtere en hendelse som pågår, eller dersom offentliggjøring av hendelsen ellers er i offentlighetens interesse.

8. Kommisjonen skal vedta gjennomføringsrettsakter for å angi nærmere elementene som er nevnt i nr. 1 og parametrene som er oppført i nr. 4 i denne artikkel. Disse gjennomføringsrettsaktene skal vedtas etter framgangsmåten med undersøkelseskomité nevnt i artikkel 22 nr. 2 innen 9. august 2017.

9. Kommisjonen kan vedta gjennomføringsrettsakter om fastsettelse av formater og framgangsmåter som får anvendelse på meldingskrav. Disse gjennomføringsrettsaktene skal vedtas etter framgangsmåten med undersøkelseskomité 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]).

Artikkel 17

Gjennomføring og håndheving

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

([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).

UOFFISIELL OVERSETTELSE

2. Med henblikk på nr. 1 skal vedkommende myndigheter ha de nødvendige fullmakter og virkemidler til å kreve at tilbydere av digitale tjenester

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

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

3. Dersom en tilbyder av digitale tjenester har sitt hovedforetak eller en representant i en medlemsstat, men sine nett- og informasjonssystemer i en eller flere andre medlemsstater, skal vedkommende myndighet i medlemsstaten der hovedforetaket eller representanten befinner seg og vedkommende myndigheter i de andre medlemsstatene samarbeide og bistå hverandre ved behov. Nevnte bistand og samarbeid kan omfatte utveksling av opplysninger mellom de berørte vedkommende myndigheter og anmodninger om å treffe tilsynstiltakene nevnt i nr. 2.

Artikkel 18

Jurisdiksjon og territorialitetsprinsippet

1. For dette direktivs formål skal en tilbyder av digitale tjenester anses å være underlagt jurisdiksjonen i den medlemsstat hvor den har sitt hovedforetak. En tilbyder av digitale tjenester skal anses å ha sitt hovedforetak i en medlemsstat når den har sitt hovedkontor i denne medlemsstaten.

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

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

KAPITTEL VI

STANDARDISERING OG FRIVILLIG MELDING

Artikkel 19

Standardisering

1. For å fremme en ensartet gjennomføring av artikkel 14 nr. 1 og 2 og artikkel 16 nr. 1 og 2 skal medlemsstatene, uten å pålegge eller innebære forskjellsbehandling til fordel for bruk av en bestemt type teknologi, oppmuntre til bruk av europeiske eller internasjonalt anerkjente standarder og spesifikasjoner som er relevante for sikkerheten i nett- 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 om allerede eksisterende standarder, herunder medlemsstatenes nasjonale standarder, som vil gjøre det mulig å dekke disse områdene.

Artikkel 20

Frivillig melding

1. Uten at det berører artikkel 3 kan foretak som ikke er blitt identifisert som ytere av samfunnsviktige tjenester, og som ikke er tilbydere av digitale tjenester, på frivillig grunnlag melde hendelser som virker betydelig inn på kontinuiteten i tjenestene de yter.

2. Når medlemsstatene behandler meldinger, skal de opptre etter framgangsmåten fastsatt i artikkel 14. Medlemsstatene kan prioritere behandlingen av obligatoriske meldinger over frivillige meldinger. Frivillige meldinger skal behandles bare dersom slik behandling ikke utgjør en uforholdsmessig stor eller urimelig byrde for medlemsstatene.

UOFFISIELL OVERSETTELSE

Frivillig melding skal ikke innebære at melderforetaket pålegges eventuelle forpliktelser som det ikke hadde vært omfattet av dersom det ikke hadde gitt meldingen.

KAPITTEL VII

SLUTTBESTEMMELSER

Artikkel 21

Sanksjoner

Medlemsstatene skal fastsette regler for sanksjoner mot overtredelser av de nasjonale bestemmelsene som er vedtatt i henhold til dette direktiv, og treffe alle nødvendige tiltak for å sikre at de gjennomføres. De fastsatte sanksjonene skal være virkningsfulle, stå i forhold til overtredelsen og virke avskrekkende. Medlemsstatene skal innen 9. mai 2018 underrette Kommisjonen om disse bestemmelsene og tiltakene og umiddelbart underrette den om eventuelle senere endringer.

Artikkel 22

Komitéframgangsmåte

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

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

Artikkel 23

Gjennomgåelse

1. Innen 9. mai 2019 skal Kommisjonen framlegge en rapport for Europaparlamentet og Rådet med en vurdering av sammenhengen i metoden som medlemsstatene har truffet med hensyn til identifisering av ytere av samfunnsviktige tjenester.

2. Kommisjonen skal regelmessig gjennomgå virkningen av dette direktiv og framlegge en rapport for Europaparlamentet og Rådet. For dette formål, og med sikte på en ytterligere fremming av strategisk og driftsmessig samarbeid, skal Kommisjonen ta hensyn til rapportene fra Samarbeidsgruppen og CSIRT-nettet om de erfaringer som er gjort på strategisk og driftsmessig plan. I sin gjennomgåelse skal Kommisjonen også vurdere listene i vedlegg II og III, og sammenhengen i identifiseringen av ytere av samfunnsviktige tjenester og 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 med sikte på å gi medlemsstatene ytterligere muligheter til hensiktsmessig samarbeid i løpet av perioden for innarbeiding i nasjonal lovgivning, skal Samarbeidsgruppen og CSIRT-nettet 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, og med henblikk på å støtte medlemsstatene i å bruke en konsekvent metode for å identifisere ytere av samfunnsviktige tjenester, skal Samarbeidsgruppen drøfte framgangsmåten for, innholdet i og typen av nasjonale tiltak som gjør det mulig å identifisere ytere av samfunnsviktige tjenester innenfor en bestemt sektor i samsvar med kriteriene fastsatt i artikkel 5 og 6. Samarbeidsgruppen skal også, på anmodning fra en medlemsstat, drøfte særlige utkast til nasjonale tiltak i medlemsstaten som gjør det mulig å identifisere ytere av samfunnsviktige tjenester innenfor en bestemt sektor i samsvar med kriteriene fastsatt i artikkel 5 og 6.

3. Innen 9. februar 2017 og ved anvendelsen av denne artikkel skal medlemsstatene sikre hensiktsmessig representasjon i

UOFFISIELL OVERSETTELSE

Samarbeidsgruppen og CSIRT-nettet.

Artikkel 25

Innarbeiding i nasjonal lovgivning

1. Medlemsstatene skal innen 9. mai 2018 vedta og kunngjøre de lover og forskrifter som er nødvendige for å etterkomme dette direktiv. 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 direktiv, 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 bestemmelser som de vedtar på det området dette direktiv omhandler.

Artikkel 26

Ikrafttredelse

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

Artikkel 27

Adressater

Dette direktiv er rettet til medlemsstatene.

Utferdiget i Strasbourg 6. juli 2016.

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

UOFFISIELL OVERSETTELSE

VEDLEGG I

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

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

1) Krav til CSIRT-enheter:

   a) CSIRT-enheter skal sikre et høyt tilgjengelighetsnivå for kommunikasjonstjenestene sine ved å unngå svake punkter («single points of failure»), og skal til enhver tid ha flere muligheter for å bli kontaktet og til å kontakte andre. Videre skal kommunikasjonskanalene tydelig angis og være godt kjent for brukergruppen og samarbeidspartnere.

   b) CSIRT-enhetenes lokaler og underliggende informasjonssystemer skal være plassert på et sikkert sted.

   c) Kontinuitet i virksomheten:

      i) CSIRT-enheter skal være utstyrt med et egnet system for å håndtere og videreformidle anmodninger, for 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 formål skal overflødige systemer og reservearbeidsområder være tilgjengelige.

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

2) CSIRT-enhetenes oppgaver:

   a) CSIRT-enhetenes oppgaver skal minst omfatte følgende:

      i) overvåke hendelser på nasjonalt plan,

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

      iii) iverksette tiltak ved hendelser,

      iv) sørge for dynamisk risiko- og hendelsesanalyse og situasjonsforståelse,

      v) delta i CSIRT-nettene.

   b) CSIRT-enheter skal inngå et 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) prosedyrer for håndtering av hendelser og risikoer,

      ii) systemer for klassifisering av hendelser, risikoer og opplysninger.

UOFFISIELL OVERSETTELSE

VEDLEGG II

TYPER AV FORETAK MED HENBLIKK PÅ ARTIKKEL 4 NR. 4

Sektor	Delsektor	Type foretak
1. Energi	a) Elektrisitet:	– Elektrisitetsforetak som definert i artikkel 2 nr. 35 i europaparlaments- og rådsdirektiv 2009/72/EF[1], som ivaretar «forsyning» i henhold til definisjonen i artikkel 2 nr. 19 i nevnte direktiv
		– Operatører av distribusjonsnett som definert i artikkel 2 nr. 6 i direktiv 2009/72/EF
		– Operatører av overføringsnett 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 transport 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 overføringsnett som definert i artikkel 2 nr. 4 i direktiv 2009/73/EF
		– Operatører av lagringsnett 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

UOFFISIELL OVERSETTELSE

Sektor	Delsektor	Type foretak
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 nevnte direktiv, herunder de viktigste lufthavnene oppført i avsnitt 2 i vedlegg II til europaparlaments- og rådsforordning (EU) nr. 1315/2013([5]), og foretak som driver tilhørende anlegg i lufthavner
		– 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	– Infrastrukturforvaltninger 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])

UOFFISIELL OVERSETTELSE

Sektor	Delsektor	Type foretak
3. Bankvirksomhet		– Kredittinstitusjoner som definert i artikkel 4 nr. 1 i europaparlaments- og rådsforordning (EU) nr. 575/2013([13])
4. Finansmarkedenes 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])
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 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

UOFFISIELL OVERSETTELSE

Sektor	Delsektor	Type foretak

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).

UOFFISIELL OVERSETTELSE

VEDLEGG III

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

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

UOFFISIELL OVERSETTELSE