Resumé af udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse om Kommissionens og Den Europæiske Unions højtstående repræsentant for udenrigsanliggender og sikkerhedspolitiks fælles meddelelse om en »EU-strategi for cybersikkerhed: Et åbent, sikkert og beskyttet cyberspace« og om Kommissionens forslag til et direktiv om foranstaltninger, der skal sikre et højt fælles niveau for net- og informationssikkerhed i hele EU

(Denne udtalelse findes i fuld udgave på EN, FR og DE på EDPS' hjemmeside under: http://www.edps.europa.eu)

(2014/C 32/10)

1. **Indledning**

1.1. *Høring af EDPS*

1. Den 7. februar 2013 vedtog Kommissionen og Den Europæiske Unions højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik en fælles meddelelse til Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget om en »EU-strategi for cybersikkerhed: Et åbent, sikkert og beskyttet cyberspace« ([1]) (herefter »den fælles meddelelse«, »strategien for cybersikkerhed« eller »strategien«).

2. Samme dag vedtog Kommissionen et forslag til Europa-Parlamentets og Rådets direktiv om foranstaltninger, der skal sikre et højt fælles niveau for net- og informationssikkerhed i hele EU ([2]) (herefter »direktivforslaget« eller »forslaget«). Forslaget blev sendt til høring hos EDPS den 7. februar 2013.

3. Inden vedtagelsen af den fælles meddelelse og af forslaget fik EDPS mulighed for at fremsætte uformelle bemærkninger til Kommissionen. EDPS glæder sig over, at nogle af disse bemærkninger er medtaget i den fælles meddelelse og i forslaget.

4. **Konklusioner**

74. EDPS glæder sig over, at Kommissionen og EU's højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik har fremlagt en omfattende strategi for cybersikkerhed suppleret af et direktivforslag om foranstaltninger, der skal sikre et højt fælles niveau for net- og informationssikkerhed (NIS) i hele EU. Strategien supplerer de politiske tiltag, som EU allerede har iværksat inden for net- og informationssikkerhed.

75. EDPS glæder sig over, at strategien går længere end den traditionelle fremgangsmåde med at stille sikkerhed op mod privatlivets fred ved at indeholde bestemmelser om udtrykkelig anerkendelse af privatlivets fred og databeskyttelse som grundlæggende værdier, der skal være retningsgivende for politikken om cybersikkerhed i EU og på verdensplan. EDPS bemærker, at strategien om cybersikkerhed og direktivforslaget om NIS kan komme til at spille en afgørende rolle med hensyn til at bidrage til at sikre beskyttelsen af fysiske personers ret til privatlivets fred og databeskyttelse i onlinemiljøet. Det skal samtidig sikres, at disse tiltag ikke munder ud i foranstaltninger, som vil udgøre ulovlige indgreb i fysiske personers ret til privatlivets fred og databeskyttelse.

76. EDPS glæder sig ligeledes over, at databeskyttelse er nævnt adskillige steder i strategien og er medtaget i direktivforslaget om NIS. EDPS beklager imidlertid, at der i strategien og direktivforslaget ikke i højere grad er foretaget en fremhævelse af den nuværende og kommende databeskyttelseslovgivnings bidrag til sikkerhed, og at det i disse dokumenter ikke fuldt ud sikres, at enhver forpligtelse, der følger af direktivforslaget eller øvrige elementer af strategien, supplerer databeskyttelsesforpligtelserne og ikke overlapper eller modsiger hinanden.

77. EDPS bemærker desuden, at strategien om cybersikkerhed som følge af manglende hensyntagen og det forhold, at der ikke fuldt ud tages højde for andre parallelle initiativer fra Kommissionen og igangværende lovgivningsprocedurer, som f.eks. databeskyttelsesreformen og den foreslåede forordning om elektroniske identifikationstjenester og tillidstjenester, ikke giver et virkelig dækkende og holistisk overblik over

([1]) JOIN(2013) 1 final.
([2]) COM(2013) 48 final.

cybersikkerheden i EU og risikerer at forfølge en diffus og skarpt opdelt strategi. EDPS bemærker ligeledes, at det foreslåede direktiv om NIS heller ikke muliggør en sammenhængende sikkerhedsstrategi i EU endnu, og at den forpligtelse, der er fastlagt i databeskyttelseslovgivningen, sandsynligvis er den mest omfattende net- og sikkerhedsforpligtelse inden for rammerne af EU-lovgivningen.

78. EDPS beklager ligeledes, at der heller ikke tages højde for databeskyttelsesmyndighedernes væsentlige rolle med hensyn til gennemførelsen og håndhævelsen af sikkerhedsforpligtelserne og forbedringen af cybersikkerhed.

79. Med hensyn til strategien om cybersikkerhed understreger EDPS følgende:

— Det er særlig vigtigt med en præcis definition af begreberne »cyberrobusthed«, »cyberkriminalitet« og »cyberforsvar«, eftersom disse begreber benyttes som en begrundelse for visse særlige foranstaltninger, som kan medføre indgreb i grundlæggende rettigheder, herunder retten til privatlivets fred og databeskyttelse. Strategiens og konventionen om internetkriminalitets definitioner af »cyberkriminalitet« er imidlertid stadig meget brede. Det vil være tilrådeligt at udarbejde en præcis og *snæver* definition af »cyberkriminalitet« i stedet for en overordnet definition.

— Databeskyttelseslovgivningen skal finde anvendelse på alle strategiens tiltag, når disse vedrører foranstaltninger, der indebærer behandling af personoplysninger. Selv om databeskyttelseslovgivningen ikke er nævnt specifikt i de afsnit, der vedrører cyberkriminalitet og cyberforsvar, fremhæver EDPS, at mange af de tiltag, der er planlagt inden for disse områder, vil komme til at omfatte behandling af personoplysninger og derfor vil være omfattet af anvendelsesområdet for den gældende databeskyttelseslovgivning. EDPS bemærker ligeledes, at mange tiltag omfatter etablering af koordinationsmekanismer, hvilket vil kræve overholdelse af passende databeskyttelsesgarantier for så vidt angår metoderne til udveksling af personoplysninger.

— Databeskyttelsesmyndighederne spiller en vigtig rolle med hensyn til cybersikkerhed. Databeskyttelsesmyndighederne deltager i deres egenskab af vogtere af fysiske personers ret til privatlivets fred og databeskyttelsesrettigheder aktivt i beskyttelsen af deres personoplysninger både på og uden for internettet. De bør derfor inddrages behørigt i deres egenskab af tilsynsorganer med hensyn til gennemførelsen af foranstaltninger, der indebærer behandling af personoplysninger (som f.eks. lanceringen af EU's pilotprojekt om bekæmpelse af botnets og malware). De øvrige medspillere inden for cybersikkerhed bør ligeledes samarbejde med dem om udførelsen af deres opgaver, f.eks. med hensyn til udveksling af bedste praksis og bevidtgørelsesaktioner. EDPS og de nationale databeskyttelsesmyndigheder bør ligeledes inddrages behørigt i den konference på højt niveau, som vil blive afholdt i 2014, og som har til formål at vurdere fremskridtet med hensyn til gennemførelsen af strategien.

80. For så vidt angår direktivforslaget om NIS tilråder EDPS lovgiverne:

— at skabe mere klarhed og sikkerhed i artikel 3, stk. 8, om definitionen af de markedsoperatører, der er omfattet af forslagets anvendelsesområde, og at udarbejde en udtømmende liste, der omfatter alle de relevante interessenter, med henblik på at sikre en fuldt ud harmoniseret og integreret tilgang til sikkerhed i EU,

— at præcisere i artikel 1, stk. 2, litra c), at direktivforslaget finder anvendelse på EU-institutioner og -organer, og medtage en henvisning til forordning (EF) nr. 45/2001 i forslagets artikel 1, stk. 5,

— at tildele dette forslag en mere horisontal funktion, for så vidt angår sikkerhed, ved udtrykkeligt at fastslå i artikel 1, at forslaget ikke berører nuværende eller fremtidige mere detaljerede regler inden for specifikke områder (som f.eks. de regler, der vil blive fastlagt med hensyn til udbydere af tillidstjenester, i den foreslåede forordning om elektroniske identifikationstjenester),

— at tilføje en betragtning, hvori der redegøres for nødvendigheden af at integrere databeskyttelse allerede på det tidlige udviklingsstadie for de i forslaget omhandlede mekanismer og i hele den livscyklus, der kendetegner de relevante processer, procedurer, organisationer, teknikker og infrastrukturer, dog under hensyntagen til den foreslåede forordning om databeskyttelse,

— at præcisere definitionen af »net- og informationssystem« i artikel 3, stk. 1, og af »hændelse« i artikel 3, stk. 4, og erstatte forpligtelsen i artikel 5, stk. 2, til at udarbejde en »risikovurderingsplan« med at »fastlægge og opretholde en risikostyringsramme«,

— at konkretisere i artikel 1, stk. 6, at behandlingen af personoplysninger er berettiget i henhold til artikel 7, litra e) i direktiv 95/46/EF, hvis dette er nødvendigt for at opfylde de mål af almen interesse, der forfølges med dette direktiv. Der skal imidlertid sikres behørig overholdelse af nødvendigheds- og proportionalitetsprincippet, således at kun de oplysninger, der er strengt nødvendige for det mål, der skal nås, bliver behandlet,

— at fastslå i artikel 14, under hvilke omstændigheder en anmeldelse er påkrævet, samt denne anmeldelses indhold og format, herunder hvilke typer personoplysninger der skal meddeles, og hvorvidt og i hvilket omfang anmeldelsen og dens ledsagedokumenter vil omhandle detaljerede personoplysninger, der er blevet berørt af en konkret sikkerhedshændelse (som f.eks. IP-adresser). Der skal tages højde for, at det kun bør være tilladt NIS-kompetente myndigheder at indsamle og behandle personoplysninger inden for rammerne af en sikkerhedshændelse, hvis dette er strengt nødvendigt. Forslaget bør ligeledes indeholde passende beskyttelsesforanstaltninger for at sikre en tilstrækkelig beskyttelse af de oplysninger, som behandles af NIS-kompetente myndigheder,

— at præcisere i artikel 14, at anmeldelsen af hændelser i medfør af artikel 14, stk. 2, ikke berører forpligtelsen i henhold til den gældende databeskyttelseslovgivning til at anmelde overtrædelser i forbindelse med personoplysninger. Forslaget bør indeholde en angivelse af de væsentligste aspekter af proceduren for samarbejdet mellem NIS-kompetente myndigheder og databeskyttelsesmyndigheder i sager, hvor sikkerhedshændelsen omfatter en overtrædelse i forbindelse med personoplysninger,

— at ændre artikel 14, stk. 8, således at udelukkelse af mikrovirksomheder fra anmeldelsens anvendelsesområde ikke gælder de operatører, der spiller en afgørende rolle med hensyn til levering af tjenester i informationssamfundet, herunder f.eks. i lyset af den informationstype, som de behandler (f.eks. biometriske data eller følsomme oplysninger),

— at tilføje bestemmelser i forslaget vedrørende NIS-kompetente myndigheders fremtidige udveksling af personoplysninger med andre modtagere, for at sikre, at i) personoplysninger kun meddeles de modtagere, hvis behandling af oplysningerne er nødvendig for udførelsen af deres opgaver i overensstemmelse med et passende retsgrundlag, og at ii) denne type oplysninger er begrænset til det omfang, der er strengt nødvendigt for udførelsen af deres opgaver. Der skal ligeledes tages hensyn til, hvordan enheder, der formidler oplysninger til informationsudvekslingsnettet, sikrer overholdelse af princippet om formålsbegrænsning,

— at angive tidsfristen for tilbageholdelse af personoplysninger til de formål, der er fastlagt i det foreslåede direktiv, især for så vidt angår NIS-kompetente myndigheders tilbageholdelse og inden for samarbejdsnettets sikre infrastruktur,

— at erindre NIS-kompetente myndigheder om deres pligt til at give de registrerede en passende orientering om behandlingen af personoplysninger ved f.eks. at oplyse om deres politik for beskyttelse af privatlivets fred på deres websted,

— at tilføje en bestemmelse vedrørende det sikkerhedsniveau, som NIS-kompetente myndigheder skal overholde, for så vidt angår de oplysninger, der indsamles, behandles og udveksles. Der bør specifikt medtages en henvisning til sikkerhedskravene i artikel 17 i direktiv 95/46/EC, for så vidt angår NIS-kompetente myndigheders beskyttelse af personoplysninger,

— at præcisere i artikel 9, stk. 2, at kriterierne for medlemsstaternes deltagelse i det sikre informationsudvekslingsnet bør sikre, at alle deltagerne i informationsudvekslingssystemerne opretholder et højt sikkerheds- og robusthedsniveau i alle faser af behandlingen. Disse kriterier skal omfatte hensigtsmæssige fortroligheds- og sikkerhedsforanstaltninger i overensstemmelse med artikel 16 og 17 i direktiv 95/46/EF og artikel 21 og 22 i forordning (EF) nr. 45/2001. Kommissionen bør udtrykkeligt pålægges at overholde disse kriterier som følge af sin deltagelse som kontrolinstans i det sikre informationsudvekslingsnet,

— at tilføje en beskrivelse i artikel 9 af henholdsvis Kommissionens og medlemsstaternes roller og ansvarsområder i forbindelse med oprettelse, drift og vedligeholdelse af det sikre informationsudvekslingssystem og at sikre, at udviklingen af dette system gennemføres i overensstemmelse med principperne om indbygget databeskyttelse og databeskyttelse gennem indstillinger samt om indbygget sikkerhed, og

— at tilføje i artikel 13, at enhver overførsel af personoplysninger til modtagere tredjelande finder sted i overensstemmelse med artikel 25 og 26 i direktiv 95/46/EF og artikel 9 i forordning (EF) nr. 45/2001.

Udfærdiget i Bruxelles, den 14. juni 2013.

Peter HUSTINX

Den Europæiske Tilsynsførende for Databeskyttelse