Samenvatting van het advies van de Europese toezichthouder voor gegevensbescherming inzake de gezamenlijke mededeling van de Commissie en de hoge vertegenwoordiger van de Europese Unie voor Buitenlandse Zaken en Veiligheidsbeleid betreffende een Strategie inzake cyberbeveiliging van de Europese Unie: een open, veilige en beveiligde cyberspace, en inzake het voorstel van de Commissie voor een richtlijn houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen

(De volledige tekst van dit advies is beschikbaar in de Engelse, Franse en Duitse taal op de website van de Europese toezichthouder voor gegevensbescherming EDPS http://www.edps.europa.eu)

(2014/C 32/10)

1. **Inleiding**

1.1. *Raadpleging van de EDPS*

1. Op 7 februari 2013 hebben de Commissie en de hoge vertegenwoordiger van de Europese Unie voor Buitenlandse Zaken en Veiligheidsbeleid een gezamenlijke mededeling aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's aangenomen betreffende een „Strategie inzake cyberbeveiliging van de Europese Unie: een open, veilige en beveiligde cyberspace" ([1]) (hierna: „de gezamenlijke mededeling", „de strategie inzake cyberbeveiliging" of „de strategie" genoemd).

2. Op dezelfde datum heeft de Commissie een voorstel aangenomen voor een Richtlijn van het Europees Parlement en de Raad houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen ([2]) (hierna de „voorgestelde richtlijn" of „het voorstel" genoemd). Dit voorstel is op 7 februari 2013 voor raadpleging naar de EDPS gestuurd.

3. Voordat de gezamenlijke mededeling en het voorstel werden aangenomen, werd de EDPS de mogelijkheid geboden informele opmerkingen te maken bij de Commissie. Het verheugt hem dat enkele van zijn opmerkingen zijn opgenomen in de gezamenlijke mededeling en het voorstel.

4. **Conclusies**

74. Het verheugt de EDPS dat de Commissie en de hoge vertegenwoordiger van de EU voor Buitenlandse Zaken en Veiligheidsbeleid een brede strategie inzake cyberbeveiliging naar voren hebben gebracht, aangevuld door een voorstel houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging (NIB) in de Unie te waarborgen. De strategie vormt een aanvulling op reeds door de EU ontwikkelde beleidsacties op het gebied van netwerk- en informatiebeveiliging.

75. Het verheugt de EDPS dat de strategie verder gaat dan de gebruikelijke benadering waarbij beveiliging tegenover privacy wordt geplaatst, door te voorzien in de uitdrukkelijke erkenning dat de bescherming van de persoonlijke levenssfeer en van gegevens kernwaarden zijn die als richtsnoer moeten dienen voor het cyberbeveiligingsbeleid in de EU en daarbuiten. De EDPS merkt op dat de strategie inzake cyberbeveiliging en de voorgestelde NIB-richtlijn een fundamentele rol kunnen spelen in het helpen waarborgen van de rechten van personen op bescherming van hun persoonlijke levenssfeer en van hun gegevens in een online-omgeving. Tegelijkertijd moet er voor worden gezorgd dat een en ander niet leidt tot maatregelen die onwettige inperkingen inhouden van de rechten van personen op bescherming van de persoonlijke levenssfeer en van hun gegevens.

76. De EDPS is ook ingenomen met het feit dat gegevensbescherming in verscheidene onderdelen van de strategie wordt vermeld en dat hiermee rekening wordt gehouden in de voorgestelde NIB-richtlijn. Hij betreurt echter dat in de strategie en de voorgestelde richtlijn geen grotere nadruk wordt gelegd op de bijdrage aan beveiliging van bestaande en aankomende gegevensbeschermingswetgeving en dat wordt nagelaten volledig te waarborgen dat verplichtingen voortvloeiend uit de voorgestelde richtlijn of andere onderdelen van de strategie een aanvulling vormen op gegevensbeschermingsverplichtingen en elkaar niet overlappen of in tegenspraak met elkaar zijn.

77. De EDPS merkt verder op dat door het gebrek aan aandacht en aan volledige rekenschap van andere, parallelle initiatieven van de Commissie en voortgaande wetgevingsprocedures, zoals de gegevensbeschermingshervorming en de voorgestelde verordening betreffende elektronische identificatie en vertrouwensdiensten, de strategie inzake cyberbeveiliging nalaat te voorzien in een werkelijk alomvattende en holistische kijk op cyberbeveiliging in de EU en een gefragmenteerde en verdeelde aanpak dreigt te bestendigen. De

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

EDPS merkt voorts op dat de voorgestelde NIB-richtlijn evenmin ruimte biedt voor een alomvattende benadering van beveiliging in de EU en dat de verplichting die in de gegevensbeschermingswetgeving is vervat waarschijnlijk het breedste netwerk en de breedste beveiligingsverplichting op grond van EU-wetgeving is.

78. De EDPS betreurt ook dat evenmin afdoende aandacht is besteed aan de belangrijke rol van gegevensbeschermingsautoriteiten in de tenuitvoerlegging en de handhaving van gegevensbeschermingsverplichtingen en in het verbeteren van cyberbeveiliging.

79. Wat de strategie inzake cyberbeveiliging betreft, benadrukt de EDPS dat:

— een duidelijke omschrijving van de termen „veerkrachtige cyberspace", „cybercriminaliteit" en „cyberdefensie" bijzonder belangrijk is omdat deze termen worden gebruikt als rechtvaardiging voor bepaalde speciale maatregelen die een inperking inhouden van grondrechten, waaronder de rechten op bescherming van de persoonlijke levenssfeer en op gegevensbescherming. De omschrijvingen van „cybercriminaliteit" in de strategie en in het Verdrag inzake cybercriminaliteit zijn erg breed gehouden. Het is aan te raden om een duidelijke en *goed afgebakende* omschrijving van „cybercriminaliteit" te hebben, in plaats van een te verreikende;

— gegevensbescherming moet gelden voor alle acties van de strategie indien zij betrekking hebben op maatregelen die de verwerking van persoonsgegevens inhouden. Hoewel gegevensbeschermingswetgeving niet specifiek wordt vermeld in de paragrafen die betrekking hebben op cybercriminaliteit en cyberdefensie, onderstreept de EDPS dat veel van de geplande inspanningen op die gebieden de verwerking van persoonsgegevens inhouden en daardoor vallen binnen de reikwijdte van de gegevensbeschermingswetgeving. Hij merkt voorts op dat veel acties bestaan uit het opzetten van coördinatiemechanismen. Deze vereisen dat er passende gegevensbeschermingswaarborgen worden verwezenlijkt aangaande de modaliteiten voor de uitwisseling van persoonsgegevens;

— gegevensbeschermingsautoriteiten een belangrijke rol spelen binnen cyberbeveiliging. Als hoedsters van de rechten op bescherming van zowel de persoonlijke levenssfeer als van persoonsgegevens, zijn gegevensbeschermingsautoriteiten actief betrokken bij de bescherming van persoonsgegevens, zowel offline als online. Ze moeten daarom als toezichthoudende organen naar behoren worden betrokken bij de tenuitvoerlegging van maatregelen die de verwerking van persoonsgegevens inhouden (zoals de lancering van een EU-proefproject ter bestrijding van botnets en malware). Andere spelers op het gebied van cyberbeveiliging moeten ook met hen samenwerken bij de uitvoering van hun taken, bijvoorbeeld de uitwisseling van beste praktijken en bewustmakingsacties. De EDPS en nationale gegevensbeschermingsautoriteiten moeten op passende wijze worden betrokken bij de conferentie op hoog niveau die in 2014 wordt belegd om de voortgang met de tenuitvoerlegging van de strategie te evalueren.

80. Wat de voorgestelde NIB-richtlijn betreft, adviseert de EDPS de wetgevers om:

— in artikel 3, lid 8, meer duidelijkheid en zekerheid te verschaffen over de omschrijving van de marktdeelnemers die vallen binnen de reikwijdte van het voorstel, en om een uitgebreide lijst op te stellen die alle relevante belanghebbenden omvat, teneinde te zorgen voor een volledig geharmoniseerde en geïntegreerde aanpak van beveiliging binnen de EU;

— in artikel 1, lid 2, onder c) te verduidelijken dat de voorgestelde richtlijn van toepassing is op EU-instellingen en organen, en in artikel 1, lid 5, van het voorstel een verwijzing op te nemen naar Verordening (EG) nr. 45/2001;

— een meer horizontale rol voor dit voorstel ten aanzien van beveiliging toe te kennen, door in artikel 1 expliciet te bepalen dat het onverminderd van toepassing is op bestaande of toekomstige, meer uitgebreide regels op specifieke gebieden (zoals uit te vaardigen regels ten aanzien van aanbieders van vertrouwensdiensten in de voorgestelde verordening betreffende elektronische identificatie);

— een overweging toe te voegen waarin de noodzaak wordt uitgelegd om specifiek ingebouwde en standaard-gegevensbescherming in te bedden, en zulks reeds in een vroeg ontwerpstadium van de in het voorstel vastgestelde mechanismen en gedurende de gehele levenscyclus van betrokken processen, procedures, organisaties, technieken en infrastructuren, met inachtneming van de voorgestelde verordening gegevensbescherming;

— de omschrijvingen „netwerk- en informatiesysteem" in artikel 3, lid 1, en van „incident" in artikel 3, lid 4 te verduidelijken en in artikel 5, lid 2 de verplichting om een „risicobeoordelingsplan" vast te stellen te vervangen door „het opzetten en in stand houden van een risicobeheerskader";

— in artikel 1, lid 6, te specificeren dat de verwerking van persoonsgegevens gerechtvaardigd is uit hoofde van artikel 7, onder e), van Richtlijn 95/46/EG voor zover het nodig is om de in de voorgestelde richtlijn nagestreefde doelstellingen van algemeen belang te verwezenlijken. De eerbiediging van de beginselen van noodzakelijkheid en evenredigheid dient echter te worden gewaarborgd, zodat alleen de gegevens die strikt noodzakelijk zijn om de doelstelling te verwezenlijken worden verwerkt;

— in artikel 14 de voorwaarden waaronder een melding vereist is vast te leggen, alsmede de inhoud en het formaat van de melding, waaronder de soorten persoonsgegevens die moeten worden gemeld en of de melding en haar ondersteunende documenten al dan niet en zo ja in welke mate bijzonderheden bevat van persoonsgegevens waarop een specifiek beveiligingsincident betrekking heeft (zoals IP-adressen). Er moet rekenschap worden gegeven van het feit dat bevoegde NIB-autoriteiten alleen persoonsgegevens in het kader van een beveiligingsincident mogen verzamelen en verwerken wanneer dit strikt noodzakelijk is. Er moeten passende waarborgen in het voorstel worden opgenomen om te zorgen voor adequate bescherming van de gegevens die door de bevoegde NIB-autoriteiten worden verwerkt;

— in artikel 14 te verduidelijken dat incidentmeldingen zoals bedoeld in artikel 14, lid 2, onverminderd vallen onder de meldingsplicht van inbreuken in verband met persoonsgegevens, ingevolge toepasselijke gegevensbeschermingswetgeving. In het voorstel moeten de voornaamste aspecten worden opgenomen van de procedure voor samenwerking van bevoegde NIB-autoriteiten met gegevensbeschermingsautoriteiten in gevallen waarbij het beveiligingsincident betrekking heeft op een inbreuk in verband met persoonsgegevens;

— artikel 14, lid 8, zodanig te wijzigen dat de uitsluiting van micro-ondernemingen van de werkingssfeer van de melding niet geldt voor deelnemers die een cruciale rol spelen in de levering van informatiemaatschappijdiensten, bijvoorbeeld gezien de aard van de informatie die zij verwerken (bijvoorbeeld biometrische of gevoelige gegevens);

— bepalingen aan het voorstel toe te voegen ter regulering van verdere uitwisselingen van persoonsgegevens door bevoegde NIB-autoriteiten met andere ontvangers, om ervoor te zorgen dat i) persoonsgegevens alleen worden vrijgegeven aan ontvangers indien verwerking nodig is voor de uitvoering van hun taken volgens een deugdelijke rechtsgrondslag en ii) dergelijke samenwerking beperkt blijft tot wat nodig is voor de uitvoering van hun taken. Er moet ook worden gelet op de wijze waarop organisaties die gegevens leveren aan het netwerk voor informatie-uitwisseling zorgen voor naleving van het beginsel van doelafbakening;

— een tijdlimiet aan te geven voor het bewaren van persoonsgegevens voor de in de voorgestelde richtlijn vermelde doelen, in het bijzonder als het gaat om het bewaren van dergelijke gegevens door bevoegde NIB-autoriteiten en binnen de beveiligingsinfrastructuur van het samenwerkingsnetwerk;

— de bevoegde NIB-autoriteiten te herinneren aan hun plicht om betrokkenen deugdelijke informatie te verschaffen over de verwerking van persoonsgegevens, bijvoorbeeld door een privacybeleid op hun website te publiceren;

— een bepaling toe te voegen ten aanzien van het beveiligingsniveau waaraan bevoegde NIB-autoriteiten dienen te voldoen met betrekking tot verzamelde, verwerkte en uitgewisselde informatie. Er moet een specifieke verwijzing naar de beveiligingsvereisten van artikel 17 van Richtlijn 95/46/EG worden opgenomen met betrekking tot de bescherming van persoonsgegevens door bevoegde NIB-autoriteiten;

— in artikel 9, lid 2, te verduidelijken dat de criteria voor de deelname van lidstaten aan het beveiligde informatie-uitwisselingsnetwerk ervoor moeten zorgen dat het niveau van beveiliging en veerkracht door alle deelnemers aan informatie-uitwisselingssystemen in alle verwerkingsstadia worden gewaarborgd. Deze criteria moeten passende maatregelen op het gebied van vertrouwelijkheid en beveiliging omvatten, overeenkomstig artikelen 16 en 17 van Richtlijn 95/46/EG en artikelen 21 en 22 van Verordening (EG) nr. 45/2001. De Commissie dient uitdrukkelijk gebonden te zijn aan deze criteria voor wat betreft haar deelname als voor de gegevensverwerking verantwoordelijke in het beveiligde informatie-uitwisselingssysteem;

— in artikel 9 een beschrijving toe te voegen van de taken en verantwoordelijkheden van de Commissie en de lidstaten bij het opzetten, gebruiken en in stand houden van het informatie-uitwisselingssysteem en te bepalen dat het systeem moet worden ontworpen volgens de beginselen van ingebouwde en standaard-gegevensbescherming en van ingebouwde beveiliging; en

— in artikel 13 toe te voegen dat elke overdracht van persoonsgegevens aan ontvangers in landen buiten de EU dient te geschieden in overeenstemming met de artikelen 25 en 26 van Richtlijn 95/46/EG en artikel 9 van Verordening (EG) Nr. 45/2001.

Gedaan te Brussel, 14 juni 2013.

Peter HUSTINX

Europese Toezichthouder voor gegevensbescherming