Sammanfattning av Europeiska datatillsynsmannens yttrande om det gemensamma meddelandet från kommissionen och Europeiska unionens höga representant för utrikes frågor och säkerhetspolitik om EU:s strategi för cybersäkerhet: en öppen, säker och trygg cyberrymd, och om kommissionens förslag till direktiv om åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet i hela unionen

(Den fullständiga texten i detta yttrande finns på engelska, franska och tyska på Europeiska datatillsynsmannens webbplats http://www.edps.europa.eu)

(2014/C 32/10)

1. **Inledning**

1.1 *Samråd med Europeiska datatillsynsmannen*

1. Den 7 februari 2013 antog kommissionen och Europeiska unionens höga representant för utrikes frågor och säkerhetspolitik ett gemensamt meddelande till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén och Regionkommittén om EU:s strategi för cybersäkerhet: en öppen, säker och trygg cyberrymd ([1]) (nedan kallat *det gemensamma meddelandet*, *cybersäkerhetsstrategin* eller *strategin*).

2. Samma dag antog kommissionen ett förslag till Europaparlamentets och rådets direktiv om åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet i hela unionen ([2]) (nedan kallat *förslaget till direktiv* eller *förslaget*). Förslaget skickades till Europeiska datatillsynsmannen för samråd den 7 februari 2013.

3. Innan det gemensamma meddelandet och förslaget antogs fick Europeiska datatillsynsmannen möjlighet att lämna informella synpunkter till kommissionen. Europeiska datatillsynsmannen välkomnar att en del av dessa synpunkter har beaktats i det gemensamma meddelandet och i förslaget.

4. **Slutsatser**

74. Europeiska datatillsynsmannen välkomnar att kommissionen och Europeiska unionens höga representant för utrikes frågor och säkerhetspolitik har lagt fram en omfattande strategi för cybersäkerhet, som kompletteras med ett förslag till direktiv om åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet i hela unionen. Strategin kompletterar de politiska åtgärder som redan har utformats av EU på området nät- och informationssäkerhet.

75. Europeiska datatillsynsmannen välkomnar att strategin går utöver det traditionella synsättet att ställa säkerhet mot integritet, genom ett uttryckligt erkännande av att integritets- och uppgiftsskydd utgör kärnvärden som bör prägla cybersäkerhetspolitiken inom EU och internationellt. Europeiska datatillsynsmannen konstaterar att cybersäkerhetsstrategin och det föreslagna direktivet om nät- och informationssäkerhet kan fylla en central funktion för att garantera skyddet av individens rätt till integritets- och uppgiftsskydd i internetmiljön. Samtidigt måste det säkerställas att strategin och förslaget inte ger upphov till åtgärder som skulle utgöra olagliga ingrepp i individens rätt till integritet och dataskydd.

76. Europeiska datatillsynsmannen välkomnar också att uppgiftsskydd nämns i flera delar av strategin och beaktas i det föreslagna direktivet. Han beklagar dock att den befintliga och kommande uppgiftsskyddslagstiftningens bidrag till säkerheten inte framhålls tydligare i strategin och förslaget till direktiv, och att det inte säkerställs fullständigt att eventuella skyldigheter till följd av det föreslagna direktivet eller andra element i strategin kompletterar uppgiftsskyddsskyldigheterna och inte överlappar eller strider mot varandra.

77. Europeiska datatillsynsmannen konstaterar dessutom att man inte beaktar och tar fullständig hänsyn till andra parallella initiativ från kommissionen och pågående lagstiftningsförfaranden, såsom reformen av uppgiftsskyddslagstiftningen och förslaget till förordning om elektronisk identifiering och betrodda tjänster, vilket innebär att cybersäkerhetsstrategin inte ger en verkligt allsidig och heltäckande bild av cybersäkerheten

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

i EU och dessutom medför en risk för en fragmenterad och uppdelad strategi. Europeiska datatillsynsmannen konstaterar vidare att förslaget till direktiv ännu inte möjliggör en allsidig säkerhetsstrategi i EU, och att den skyldighet som anges i dataskyddslagstiftningen förmodligen är den mest omfattande nät- och säkerhetsskyldigheten i EU:s lagstiftning.

78. Europeiska datatillsynsmannen beklagar likaså att dataskyddsmyndigheternas viktiga roll i genomförandet och verkställandet av säkerhetsskyldigheter och främjande av cybersäkerhet inte heller övervägs på lämpligt sätt.

79. När det gäller cybersäkerhetsstrategin understryker Europeiska datatillsynsmannen följande:

— En tydlig definition av begreppen ”cyberberedskap”, ”cyberbrottslighet” och ”cyberförsvar” är särskilt viktig eftersom dessa begrepp används som en motivering för vissa specialområden som kan inkräkta på de grundläggande rättigheterna, inklusive rätten till integritet och dataskydd. De definitioner av ”cyberbrottslighet” som anges i strategin och i konventionen om it-brottslighet förblir emellertid mycket allmänna. Det är tillrådligt att ha en tydlig och *restriktiv* definition av cyberbrottslighet i stället för en övergripande definition.

— Dataskyddslagstiftningen bör gälla alla åtgärder i strategin när de rör åtgärder som medför behandling av personuppgifter. Även om dataskyddslagstiftningen inte nämns uttryckligen i de avsnitt som handlar om cyberbrottslighet och cyberförsvar understryker Europeiska datatillsynsmannen att många av de åtgärder som planeras inom dessa områden medför behandling av personuppgifter, vilket innebär att de omfattas av den tillämpliga dataskyddslagstiftningen. Datatillsynsmannen konstaterar också att många åtgärder handlar om inrättande av samordningsmekanismer, vilket kommer att kräva genomförande av lämpliga dataskyddsgarantier för de moment som rör utbyte av personuppgifter.

— Datatillsynsmyndigheterna spelar en viktig roll på cybersäkerhetsområdet. I egenskap av väktare av individens integritets- och dataskyddsrättigheter är datatillsynsmyndigheterna aktivt engagerade i skyddet av personuppgifter, både utanför och på internet. I sin egenskap av tillsynsorgan bör de därför vara delaktiga på lämpligt sätt i genomförandet av åtgärder som omfattar behandling av personuppgifter (till exempel lanseringen av EU:s pilotprojekt för att bekämpa botnät och skadlig programvara). Dessutom bör andra aktörer på cybersäkerhetsområdet samarbeta med datatillsynsmyndigheterna när de fullgör sina uppgifter, till exempel när det gäller utbyte av bästa praxis och upplysningskampanjer. Europeiska datatillsynsmannen och de nationella datatillsynsmyndigheterna bör även delta på lämpligt sätt i den högnivåkonferens som kommer att hållas 2014 för att utvärdera framstegen med strategins genomförande.

80. När det gäller förslaget till direktiv om nät- och informationssäkerhet råder Europeiska datatillsynsmannen lagstiftarna att göra följande:

— Skapa mer klarhet och tydlighet i artikel 3.8 om definitionen av de marknadsoperatörer som omfattas av förslaget och utarbeta en uttömmande förteckning över alla berörda intressenter i syfte att garantera en fullständigt harmoniserad och integrerad säkerhetsstrategi inom EU.

— I artikel 1.2 c klargöra att förslaget till direktiv är tillämpligt på EU:s institutioner och organ, och infoga en hänvisning till förordning (EG) nr 45/2001 i artikel 1.5 i förslaget.

— Ge förslaget en mer övergripande roll med avseende på säkerhetsaspekterna genom att i artikel 1 uttryckligen ange att direktivet bör gälla utan att det påverkar framtida eller mer detaljerade regler inom specifika områden (till exempel de kommande reglerna om leverantörer av betrodda tjänster i förslaget till förordning om elektronisk identifiering).

— Lägga till ett skäl för att förklara behovet av att inbegripa inbyggt uppgiftsskydd och uppgiftsskydd som standard redan i ett tidigt skede i utformningen av de mekanismer som fastställs i förslaget och genom hela livscykeln för berörda processer, förfaranden, organisationer, tekniker och infrastrukturer, med hänsyn till den föreslagna dataskyddslagstiftningen.

— Klargöra definitionerna av ”nät- och informationssystem” i artikel 3.1 och ”incident” i artikel 3.4 samt i artikel 5.2 ersätta skyldigheten att inrätta en ”riskbedömningsplan” med ”inrättande och underhåll av en riskhanteringsram”.

— I artikel 1.6 förtydliga att behandlingen av personuppgifter är motiverad enligt artikel 7 e i direktiv 95/46/EG i den mån den är nödvändig för att tillgodose detta förslag till direktivs syfte av allmänintresse. Nödvändighets- och proportionalitetsprinciperna måste dock respekteras på vederbörligt sätt, så att endast uppgifter som är absolut nödvändiga för ändamålet får inhämtas och behandlas.

— I artikel 14 fastställa de omständigheter under vilka en anmälan krävs samt anmälans innehåll och format, inklusive de typer av personuppgifter som ska anmälas och om anmälan och de styrkande handlingarna kommer att innehålla upplysningar om personuppgifter som påverkas av en specifik säkerhetsincident (som IP-adresser) eller ej, och i så fall i vilken utsträckning. Det är också nödvändigt att ta hänsyn till att behöriga myndigheter för nät- och informationssäkerhet endast har rätt att samla in och behandla personuppgifter i samband med en säkerhetsincident när det är absolut nödvändigt. Lämpliga garantier bör också anges i förslaget för att se till att de uppgifter som behandlas av behöriga myndigheter för nät- och informationssäkerhet skyddas på lämpligt sätt.

— I artikel 14 klargöra att anmälan av incidenter i enlighet med artikel 14.2 bör gälla utan att det påverkar anmälningsskyldigheter avseende personuppgiftsbrott enligt den tillämpliga dataskyddslagstiftningen. De viktigaste aspekterna av förfarandet för samarbete mellan behöriga myndigheter för nät- och informationssäkerhet och dataskyddsmyndigheter i fall där en säkerhetsincident omfattar ett personuppgiftsbrott bör också anges i förslaget.

— Ändra artikel 14.8 så att undantagandet av mikroföretag från anmälningsskyldigheten inte gäller för de operatörer som spelar en central roll i tillhandahållandet av informationssamhällets tjänster, till exempel med tanke på karaktären hos den information de behandlar (t.ex. biometriska uppgifter eller känsliga uppgifter).

— Lägga till bestämmelser i förslaget om hur ytterligare utbyte av personuppgifter av behöriga myndigheter för nät- och informationssäkerhet ska ske, för att se till att i) personuppgifter endast lämnas ut till mottagare om behandling krävs för att de ska kunna utföra sina arbetsuppgifter enligt en lämplig rättslig grund, och ii) att sådan information begränsas till vad som krävs för att de ska kunna utföra sina arbetsuppgifter. Man bör även överväga hur de enheter som lämnar uppgifter till nätverket för informationsutbyte garanterar att principen om ändamålsbegränsning efterlevs.

— Ange tidsgränserna för lagring av personuppgifter för de ändamål som anges i förslaget till direktiv, i synnerhet vad gäller lagring av personuppgifter av behöriga myndigheter för nät- och informationssäkerhet, och inom samarbetsnätverkets säkra infrastruktur.

— Påminna behöriga myndigheter för nät- och informationssäkerhet om deras skyldighet att lämna lämplig information till registrerade, till exempel genom att offentliggöra en integritetspolicy på sin webbplats.

— Lägga till en bestämmelse om den säkerhetsnivå som behöriga myndigheter för nät- och informationssäkerhet ska uppfylla med avseende på den information som samlas in, behandlas och utbyts. En hänvisning till säkerhetskraven i artikel 17 i direktiv 95/46/EG bör särskilt infogas när det gäller skydd av personuppgifter av behöriga myndigheter för nät- och informationssäkerhet.

— I artikel 9.2 klargöra att kriterierna för medlemsstaternas deltagande i det säkra informationsutbytessystemet bör vara utformade för att garantera en hög säkerhets- och beredskapsnivå hos alla deltagare i informationsutbytessystemen i alla skeden av behandlingen. Dessa kriterier bör omfatta lämpliga sekretess- och säkerhetsåtgärder i enlighet med artiklarna 16 och 17 i direktiv 95/46/EG och artiklarna 21 och 22 i förordning (EG) nr 45/2001. Kommissionen bör uttryckligen vara bunden av dessa kriterier för sitt deltagande som registeransvarig i det säkra informationsutbytessystemet.

— I artikel 9 lägga till en beskrivning av kommissionens och medlemsstaternas roller och ansvar för inrättandet, driften och underhållet av det säkra informationsutbytessystemet och fastställa att systemet bör utformas i enlighet med principerna för inbyggt uppgiftsskydd och uppgiftsskydd som standard.

— I artikel 13 lägga till en bestämmelse om att all överföring av personuppgifter till mottagare i länder utanför EU ska ske i enlighet med artiklarna 25 och 26 i direktiv 95/46/EG och artikel 9 i förordning (EG) nr 45/2001.

Utfärdat i Bryssel den 14 juni 2013.

Peter HUSTINX

Europeiska datatillsynsmannen