Tiivistelmä Euroopan tietosuojavaltuutetun lausunnosta, joka koskee komission ja Euroopan unionin ulkoasioiden ja turvallisuuspolitiikan korkean edustajan yhteistä tiedonantoa ”Euroopan unionin kyberturvallisuusstrategia: avoin, turvallinen ja vakaa verkkoympäristö” sekä komission ehdotusta direktiiviksi toimenpiteistä yhteisen korkeatasoisen verkko- ja tietoturvan varmistamiseksi koko unionissa

(Koko lausunto on luettavissa englanniksi, ranskaksi ja saksaksi Euroopan tietosuojavaltuutetun verkkosivustolla http://www.edps.europa.eu)

(2014/C 32/10)

1. **Johdanto**

1.1 *Euroopan tietosuojavaltuutetun kuuleminen*

1. Komissio ja Euroopan unionin ulkoasioiden ja turvallisuuspolitiikan korkea edustaja hyväksyivät 7 päivänä helmikuuta 2013 Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle laatimansa yhteisen tiedonannon ”Euroopan unionin kyberturvallisuusstrategia: avoin, turvallinen ja vakaa verkkoympäristö” ([1]) (jäljempänä ’yhteinen tiedonanto’, ’kyberturvallisuusstrategia’ tai ’strategia’).

2. Komissio hyväksyi samana päivänä ehdotuksen Euroopan parlamentin ja neuvoston direktiiviksi toimenpiteistä yhteisen korkeatasoisen verkko- ja tietoturvan varmistamiseksi koko unionissa ([2]) (jäljempänä ’direktiiviehdotus’ tai ’ehdotus’). Ehdotus toimitettiin 7 päivänä helmikuuta 2013 Euroopan tietosuojavaltuutetulle lausuntoa varten.

3. Tietosuojavaltuutetulla oli mahdollisuus esittää komissiolle epävirallisia huomautuksia ennen yhteisen tiedonannon ja ehdotuksen hyväksymistä. Tietosuojavaltuutettu on tyytyväinen siihen, että joitakin hänen huomautuksistaan on otettu huomioon yhteisessä tiedonannossa ja ehdotuksessa.

4. **Päätelmät**

74. Tietosuojavaltuutettu on tyytyväinen siihen, että komissio ja EU:n ulkoasioiden ja turvallisuuspolitiikan korkea edustaja ovat laatineet kattavan kyberturvallisuusstrategian ja täydentäneet sitä direktiiviehdotuksella, jossa säädetään toimenpiteistä yhteisen korkeatasoisen verkko- ja tietoturvan varmistamiseksi koko EU:ssa. Strategia täydentää EU:ssa jo toteutettuja verkko- ja tietoturvapoliittisia toimenpiteitä.

75. Tietosuojavaltuutettu suhtautuu myönteisesti myös siihen, ettei strategiassa tyydytä turvallisuuden ja yksityisyyden perinteiseen vastakkainasetteluun vaan tunnustetaan nimenomaisesti, että yksityisyyden suoja ja tietosuoja ovat keskeisiä periaatteita, joiden tulisi ohjata kyberturvallisuuspolitiikkaa EU:ssa ja kansainvälisesti. Tietosuojavaltuutettu huomauttaa, että kyberturvallisuusstrategia ja ehdotettu verkko- ja tietoturvadirektiivi voivat osaltaan auttaa merkittävästi varmistamaan yksityisyyden suojan ja tietosuojan verkkoympäristössä. Samanaikaisesti on kuitenkin huolehdittava siitä, etteivät ne johda toimenpiteisiin, joilla yksityisyyden suoja ja tietosuoja vaarannetaan lainvastaisesti.

76. Tietosuojavaltuutettu on tyytyväinen myös siihen, että tietosuoja mainitaan useissa strategian kohdissa ja että se on huomioitu myös verkko- ja tietoturvaa koskevassa direktiiviehdotuksessa. Tietosuojavaltuutettu pitää kuitenkin valitettavana, ettei strategiassa ja ehdotuksessa tuoda selkeämmin esille, kuinka voimassa oleva ja tuleva tietosuojalainsäädäntö parantaa turvallisuutta, eikä myöskään kaikilta osin varmisteta, että direktiiviehdotuksesta tai strategian muista osista johtuvat velvoitteet täydentävät nykyisiä tietosuojavelvoitteita ilman päällekkäisyyksiä tai ristiriitaisuuksia.

77. Lisäksi tietosuojavaltuutettu huomauttaa, ettei kyberturvallisuusstrategian lähestymistapa kyberturvallisuuteen ole riittävän kattava ja kokonaisvaltainen, koska siinä ei ole punnittu eikä otettu kaikilta osin huomioon komission muita aloitteita ja käynnissä olevia lainsäädäntömenettelyjä, kuten tietosuojauudistusta ja sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista annettua asetusehdotusta, ja että strategia voi siten pahentaa entisestään nykyistä hajanaista ja lokeroitunutta lähestymistapaa.

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

Tietosuojavaltuutettu huomauttaa myös, ettei verkko- ja tietoturvaa koskeva direktiiviehdotus vielä sellaisenaan mahdollista kokonaisvaltaista lähestymistapaa turvallisuuteen EU:ssa ja että nykyisessä tietosuojalainsäädännössä säädetty velvoite on todennäköisesti kokonaisvaltaisin EU:n lainsäädännössä tähän mennessä asetettu verkko- ja turvallisuusvelvoite.

78. Edelleen tietosuojavaltuutettu pitää valitettavana sitä, ettei strategiassa ja ehdotuksessa ole otettu asianmukaisesti huomioon tietosuojaviranomaisten merkittävää roolia turvallisuusvelvoitteiden täytäntöönpanossa ja soveltamisen valvonnassa sekä kyberturvallisuuden parantamisessa.

79. Kyberturvallisuusstrategian osalta tietosuojavaltuutettu korostaa seuraavaa:

— ”Verkon vakauden”, ”verkkorikollisuuden” ja ”verkkopuolustuksen” käsitteiden selkeä määrittely on erityisen tärkeää, koska näillä käsitteillä perustellaan tiettyjä erityistoimenpiteitä, jotka voivat johtaa perusoikeuksien, kuten yksityisyyden suojan ja tietosuojan loukkauksiin. Strategiassa ja tietoverkkorikollisuutta koskevassa yleissopimuksessa annettu verkkorikoksen määritelmä on kuitenkin hyvin yleinen. Verkkorikoksesta olisi suotavaa käyttää mahdollisimman selkeää ja pikemminkin *rajoittavaa* kuin liian väljää määritelmää;

— Tietosuojalainsäädäntöä olisi sovellettava kaikkiin strategiaan sisältyviin toimenpiteisiin, joihin liittyy henkilötietojen käsittelyä. Vaikka tietosuojalainsäädäntöä ei mainitakaan nimenomaisesti verkkorikollisuutta ja verkkopuolustusta käsittelevissä strategian kohdissa, tietosuojavaltuutettu korostaa, että monet näillä aloilla suunnitelluista toimista edellyttävät henkilötietojen käsittelyä ja kuuluvat siten sovellettavan tietosuojalainsäädännön soveltamisalaan. Tietosuojavaltuutettu panee myös merkille, että useat näistä toimista muodostuvat koordinointijärjestelyistä, jotka edellyttävät asianmukaisten tietosuojatakeiden sisällyttämistä henkilötietojen vaihtoa koskeviin yksityiskohtaisiin sääntöihin;

— Tietosuojaviranomaisilla on keskeinen osuus kyberturvallisuuden varmistamisessa. Tietosuojaviranomaiset ovat yksityisyyden suojan ja tietosuojan valvojia, jotka osallistuvat aktiivisesti henkilötietojen suojaamiseen sekä verkossa että sen ulkopuolella. Valvontaeliminä näiden viranomaisten olisi voitava osallistua asianmukaisesti henkilötietojen käsittelyyn liittyviin täytäntöönpanotoimiin (esim. bottiverkkojen ja haittaohjelmien torjuntaa koskevan EU:n pilottihankkeen käynnistäminen). Muiden kyberturvallisuusalan toimijoiden olisi tehtävä viranomaisten kanssa yhteistyötä näiden tehtävien hoitamisessa esimerkiksi vaihtamalla parhaita käytäntöjä ja toteuttamalla toimia yleisen tietoisuuden lisäämiseksi. Tietosuojavaltuutetun ja kansallisten tietosuojaviranomaisten olisi myös voitava osallistua asianmukaisesti vuonna 2014 pidettävään korkean tason konferenssiin, jossa arvioidaan strategian täytäntöönpanon edistymistä.

80. Ehdotetun verkko- ja tietoturvadirektiivin osalta tietosuojavaltuutettu suosittelee lainsäätäjille seuraavaa:

— parannetaan ehdotuksen soveltamisalaan kuuluvien markkinatoimijoiden määritelmän selkeyttä ja varmuutta 3 artiklan 8 kohdassa ja laaditaan kaikki asiaankuuluvat sidosryhmät sisältävä tyhjentävä luettelo täysin yhdenmukaisen ja yhdennetyn lähestymistavan soveltamiseksi turvallisuuteen EU:ssa;

— täsmennetään 1 artiklan 2 kohdan c alakohdassa, että direktiiviehdotusta sovelletaan kaikkiin EU:n toimielimiin ja elimiin, ja lisätään ehdotuksen 1 artiklan 5 kohtaan viittaus asetukseen (EY) N:o 45/2001;

— korostetaan ehdotuksen laaja-alaisuutta turvallisuuden alalla säätämällä nimenomaisesti 1 artiklassa, että sitä sovelletaan sanotun kuitenkaan rajoittamatta voimassa olevien tai tulevien yksityiskohtaisten alakohtaisten sääntöjen (esim. elektronista tunnistamista koskevassa asetusehdotuksessa annettujen luottamuspalvelujen tarjoajia koskevat säännöt) soveltamista;

— lisätään ehdotukseen johdanto-osaan uusi kappale, jossa selitetään, että sisäänrakennetun ja oletusarvoisen yksityisyyden suojan periaatteita on sovellettava jo ehdotuksessa tarkoitettujen järjestelmien suunnittelun varhaisessa vaiheessa ja järjestelmiin sisältyvien prosessien, menettelyjen, organisaatioiden, tekniikoiden ja infrastruktuurien koko elinkaaren ajan tulevan tietosuoja-asetuksen mukaisesti;

— täsmennetään 3 artiklan 1 kohdassa esitettyä ”verkko- ja tietojärjestelmän” määritelmää ja 3 artiklan 4 kohdassa esitettyä ”turvapoikkeaman” määritelmää ja korvataan 5 artiklan 2 kohdassa säädetty velvollisuus laatia ”riskinhallintasuunnitelma” velvollisuudella ”toteuttaa riskinhallintajärjestelmä ja ylläpitää sitä”;

— täsmennetään 1 artiklan 6 kohdassa, että henkilötietojen käsittely voidaan hyväksyä ainoastaan direktiivin 95/46/EY 7 artiklan e kohdan nojalla edellyttäen, että se on välttämätöntä yleiseen etuun liittyvien ehdotetun direktiivin tavoitteiden kannalta. On kuitenkin varmistettava, että välttämättömyyden ja oikeasuhteisuuden periaatteita noudatetaan asianmukaisella tavalla, jotta tässä yhteydessä käsiteltäisiin ainoastaan tietoja, jotka ovat ehdottoman tarpeellisia käsittelyn tarkoituksen kannalta;

— määritellään 14 artiklassa, missä tilanteissa turvapoikkeamista ilmoittamista edellytetään, määritetään ilmoituksen muoto ja sisältö ja täsmennetään, minkä tyyppiset henkilötiedot olisi ilmoitettava ja sisältyykö ilmoitukseen ja siihen liittyviin asiakirjoihin itse turvapoikkeamaan liittyviä henkilötietoja (kuten IP-osoitteita) ja missä määrin. Lisäksi olisi huomioitava, että henkilötietojen keruu ja käsittely turvapoikkeamien yhteydessä olisi sallittava verkko- ja tietoturvasta vastaaville toimivaltaisille viranomaisille vain, jos se on ehdottoman tarpeellista. Ehdotuksessa olisi myös säädettävä asianmukaiset takeet, joilla turvataan verkko- ja tietoturvasta vastaavien toimivaltaisten viranomaisten käsittelemien tietojen asianmukainen suoja;

— täsmennetään 14 artiklassa, ettei 14 artiklan 2 kohdassa tarkoitettu velvollisuus ilmoittaa turvapoikkeamista saa rajoittaa sovellettavassa tietosuojalainsäädännössä asetettuja henkilötietojen tietoturvaloukkauksista ilmoittamista koskevia velvoitteita. Ehdotuksessa olisi säädettävä pääkohdittain verkko- ja tietoturvasta vastaavien toimivaltaisten viranomaisten ja tietosuojaviranomaisten välisestä yhteistyömenettelystä tapauksissa, joissa turvapoikkeamaan liittyy henkilötietojen tietoturvaloukkaus;

— muutetaan 14 artiklan 8 kohtaa niin, että mikroyritysten sulkeminen ilmoitusvelvollisuuden ulkopuolelle ei koske toimijoita, joilla on ratkaiseva osuus tietoyhteiskunnan palvelujen tarjoamisessa, esimerkiksi niiden käsittelemien tietojen luonteen perusteella (esim. biometriset tiedot tai arkaluonteiset tiedot);

— lisätään ehdotukseen säännökset, joita sovelletaan henkilötietojen vaihtoon verkko- ja tietoturvasta vastaavien toimivaltaisten viranomaisten ja muiden vastaanottajien välillä sen varmistamiseksi, että i) henkilötietoja luovutetaan ainoastaan sellaisille vastaanottajille, joiden on välttämättä käsiteltävä tietoja voidakseen suorittaa tehtävänsä asianmukaisen oikeusperustan nojalla ja että ii) käsittely rajoittuu ainoastaan tietoihin, jotka ovat välttämättömiä näiden tehtävien suorittamiseksi. Lisäksi olisi pohdittava, kuinka tiedonjakoverkkoon tietoja toimittavat toimijat voivat varmistaa, että käyttötarkoituksen rajoittamisen periaatetta noudatetaan;

— määritellään tarkemmin säilytysajat direktiiviehdotuksessa mainittuihin tarkoituksiin kerätyille henkilötiedoille ja erityisesti verkko- ja tietoturvasta vastaavien toimivaltaisten viranomaisten hallussa oleville ja yhteistyöverkoston suojatussa infrastruktuurissa säilytettäville tiedoille;

— muistutetaan verkko- ja tietoturvasta vastaavia toimivaltaisia viranomaisia niiden velvollisuudesta tiedottaa rekisteröidyille asianmukaisesti heidän henkilötietojensa käsittelystä esimerkiksi julkaisemalla tietosuojalauseke verkkosivustolla;

— lisätään ehdotukseen säännös turvallisuustasosta, jota verkko- ja tietoturvasta vastaavien toimivaltaisten viranomaisten on ylläpidettävä kerätessään, käsitellessään ja vaihtaessaan tietoja. Säännökseen on sisällytettävä nimenomainen viittaus direktiivin 95/46/EY 17 artiklassa tarkoitettuihin turvallisuusvaatimuksiin, joita verkko- ja tietoturvasta vastaavien toimivaltaisten viranomaisten on sovellettava henkilötietojen suojan varmistamiseksi;

— täsmennetään 9 artiklan 2 kohdassa, että jäsenvaltioiden osallistumiselle suojattuun tiedonjakojärjestelmään on asetettava kriteerit, joilla varmistetaan, että kaikki osallistujat takaavat suojatun tiedonjakojärjestelmän korkean tason turvallisuuden ja sietokyvyn käsittelyn kaikissa vaiheissa. Kriteereihin olisi sisällytettävä asianmukaiset toimenpiteet käsittelyn luottamuksellisuuden ja turvallisuuden varmistamiseksi direktiivin 95/46/EY 16 ja 17 artiklan ja asetuksen (EY) N:o 45/2001 21 ja 22 artiklan mukaisesti. Lisäksi olisi säädettävä nimenomaisesti, että nämä kriteerit sitovat komissiota sen osallistuessa rekisterinpitäjänä suojattuun tiedonjakojärjestelmään;

— Lisätään 9 artiklaan kuvaus komission ja jäsenvaltioiden tehtävistä ja vastuista suojatun tiedonjakojärjestelmän perustamisessa, toiminnassa ja ylläpidossa, ja edellytetään, että järjestelmä on suunniteltava sisäänrakennetun ja oletusarvoisen yksityisyyden suojan ja sisäänrakennetun turvallisuuden periaatteiden mukaisesti; ja

— Lisätään 13 kohtaan säännös, jonka mukaan henkilötietojen siirroissa EU:n ulkopuolisissa maissa sijaitseville vastaanottajille on noudatettava direktiivin 95/46/EY 25 ja 26 artiklaa ja asetuksen (EY) N:o 45/2001 9 artiklaa.

Tehty Brysselissä 14 päivänä kesäkuuta 2013.

Peter HUSTINX

Euroopan tietosuojavaltuutettu