Euroopan tietosuojavaltuutetun lausunto komission tiedonannosta Euroopan parlamentille ja neuvostolle ”EU:n sisäisen turvallisuuden strategian toteuttaminen: viisi askelta kohti turvallisempaa Eurooppaa”

(2011/C 101/02)

EUROOPAN TIETOSUOJAVALTUUTETTU, joka

ottaa huomioon Euroopan unionin toiminnasta tehdyn sopimuksen ja erityisesti sen 16 artiklan,

ottaa huomioon Euroopan unionin perusoikeuskirjan ja erityisesti sen 7 ja 8 artiklan,

ottaa huomioon yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 24 päivänä lokakuuta 1995 annetun Euroopan parlamentin ja neuvoston direktiivin 95/46/EY ([1]),

ottaa huomioon yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 18 päivänä joulukuuta 2000 annetun Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 45/2001 ([2]) ja erityisesti sen 41 artiklan mukaisesti tietosuojavaltuutetulle lähetetyn lausuntopyynnön,

ON ANTANUT SEURAAVAN LAUSUNNON:

I **JOHDANTO**

1. Komissio antoi 22. marraskuuta 2010 tiedonannon ”EU:n sisäisen turvallisuuden strategian toteuttamissuunnitelma: viisi askelta kohti turvallisempaa Eurooppaa” (jäljempänä ’tiedonanto’) ([3]). Tiedonanto toimitettiin Euroopan tietosuojavaltuutetulle kuulemista varten.

2. Euroopan tietosuojavaltuutettu on tyytyväinen siihen, että komissio kuuli häntä tiedonannosta. Euroopan tietosuojavaltuutettu esitti epävirallisia huomioita tiedonantoluonnoksesta jo ennen sen hyväksymistä, ja jotkin noista huomioista on otettu huomioon lopullisessa tiedonannossa.

Tiedonannon taustaa

3. Tiedonannossa käsitellään EU:n sisäisen turvallisuuden strategiaa, joka hyväksyttiin 23. helmikuuta 2010 Espanjan puheenjohtajakaudella ([4]). Strategiassa määritellään eurooppalainen turvallisuusmalli, jossa yhdistellään toimia muun muassa lainvalvonnan, oikeudellisen yhteistyön, rajaturvallisuuden ja pelastuspalvelun alalla kunnioittaen kuitenkin samalla yhteisiä eurooppalaisia arvoja, kuten perusoikeuksia. Strategian päätavoitteina on:

— esitellä kansalaisille nykyiset EU:n välineet, joilla voidaan jo taata EU:n kansalaisten turvallisuus ja vapaus, sekä osoittaa lisäarvo, jota EU:n toiminnasta saadaan tällä alalla;

— kehittää edelleen yhteisiä välineitä ja toimintamalleja soveltamalla yhtenäisempää lähestymistapaa, jossa puututaan turvattomuuden seurausten ohella myös sen syihin;

— vahvistaa lainvalvontaa, oikeudellista yhteistyötä, rajaturvallisuutta, pelastuspalvelua sekä suuronnettomuuksien hallintaa.

4. Sisäisen turvallisuuden strategian tavoitteena on torjua EU:n turvallisuuden kannalta suurimpia uhkia ja haasteita, kuten vakavaa ja järjestäytynyttä rikollisuutta, terrorismia sekä tietoverkkorikollisuutta. Lisäksi siinä pyritään lujittamaan EU:n ulkorajojen valvontaa ja vahvistamaan kykyä selviytyä sekä luonnonvoimien että ihmisen aiheuttamista katastrofeista. Strategiassa määritetään yleiset suuntaviivat, periaatteet ja ohjeet, joiden mukaisesti EU:n pitäisi toimia noilla aloilla, sekä kehotetaan komissiota antamaan ehdotuksia oikein ajoitetuista toimista strategian toteuttamiseksi.

5. Tässä yhteydessä on tärkeää mainita myös 8–9. marraskuuta 2010 pidetyn oikeus- ja sisäasioiden neuvoston päätelmät järjestäytynyttä ja vakavaa kansainvälistä rikollisuutta koskevan EU:n toimintapoliittisen syklin perustamisesta ja toteuttamisesta ([5]) (jäljempänä ’marraskuun 2010 päätelmät’). Marraskuun 2010 päätelmät ovat jatkoa neuvoston vuonna 2006 hyväksymille päätelmille sisäisen turvallisuuden rakenteista ([6]), ja niissä kehotetaan neuvostoa ja komissiota kehittämään kattava sisäisen turvallisuuden strategia, joka perustuu EU:n perusoikeuskirjassa vahvistettuihin EU:n yhteisiin arvoihin ([7]).

([1]) EYVL L 281, 23.11.1995, s. 31.
([2]) EYVL L 8, 12.1.2001, s. 1.
([3]) KOM(2010) 673 lopullinen
([4]) Asiak. 5842/2/10.
([5]) Neuvoston 3043. istunto, oikeus- ja sisäasiat, Bryssel, 8–9. marraskuuta 2010.
([6]) Asiak. 7039/2/06 JAI 86 CATS 34.
([7]) Marraskuun 2010 päätelmissä hyväksyttiin vakavaa kansainvälistä ja järjestäytynyttä rikollisuutta koskeva EU:n toimintapoliittinen sykli, joka on nelivaiheinen: 1) Toimintapolitiikan suunnittelu käyttäen perustana vakavaa ja järjestäytynyttä rikollisuutta koskevaa Euroopan unionin uhkakuva-arviota (European Union Serious and Organised Crime Threat Assessment, EU SOCTA). 2) Toimintapolitiikan määrittely ja päätöksenteko sen perusteella, että neuvosto määrittää rajoitetun määrän painopisteitä. 3) Vuotuisten operatiivisten toimintasuunnitelmien täytäntöönpano ja seuranta. 4) Toimintapoliittisen syklin päätteeksi suoritetaan perinpohjainen arviointi, joka toimii seuraavan syklin lähtökohtana.

6. Marraskuun 2010 päätelmissä luetellaan sisäisen turvallisuuden strategian toteuttamisessa olennaisia ohjeita ja tavoitteita, kuten ennakoivan ja tiedusteluperusteisen lähestymistavan kehittäminen, EU:n erillisvirastojen yhteistyön vahvistaminen ja niiden välisen tietojenvaihdon parantaminen sekä kansalaisten tietoisuuden lisääminen siitä, miten merkittävää työtä unioni tekee heidän suojelemisekseen. Marraskuun 2010 päätelmissä kehotetaan myös komissiota laatimaan asiaankuuluvien virastojen sekä jäsenvaltioiden asiantuntijoiden kanssa kullekin painopisteelle monivuotisen strategiaohjelman, jossa määritetään paras strategia kulloinkin kyseessä olevan ongelman ratkaisemista varten. Lisäksi marraskuun 2010 päätelmissä kehotetaan komissiota kuulemaan jäsenvaltioiden ja EU:n erillisvirastojen asiantuntijoita ja kehittämään sen perusteella riippumattoman mekanismin, jolla voidaan arvioida monivuotisten strategiaohjelmien toteuttamista. Euroopan tietosuojavaltuutettu palaa näihin asioihin jäljempänä tässä lausunnossa, koska ne liittyvät läheisesti tai vaikuttavat merkittävästi niin henkilötietojen suojaan, yksityisyyteen kuin muihin asiaan kuuluviin perusoikeuksiin ja -vapauksiin.

Tiedonannon sisältö ja tavoitteet

7. Tiedonannossa esitetään viisi strategista tavoitetta, jotka kaikki liittyvät yksityisyyteen ja tietosuojaan:

   — Hajotetaan kansainväliset rikollisverkostot.

   — Ehkäistään terrorismia ja radikalisoitumista ja puututaan terroristien värväystoimintaan.

   — Parannetaan kansalaisten ja yritysten turvallisuutta verkkoympäristössä.

   — Vahvistetaan turvallisuutta rajavalvonnan avulla.

   — Parannetaan Euroopan kykyä selviytyä kriiseistä ja katastrofeista.

8. Tiedonannon mukaan *sisäisen turvallisuuden strategian toteuttamissuunnitelmassa* määritetään yhteinen toimintaohjelma jäsenvaltioille, Euroopan parlamentille, komissiolle, neuvostolle, erillisvirastoille sekä muille toimijoille, kuten kansalaisyhteiskunnalle ja paikallisviranomaisille. Toteuttamissuunnitelmassa tehdään myös ehdotuksia siitä, millä tavoin edellä mainittujen pitäisi tehdä yhteistyötä seuraavien neljän vuoden aikana, jotta sisäisen turvallisuuden strategian tavoitteet voitaisiin saavuttaa.

9. Tiedonanto perustuu Lissabonin sopimukseen, ja siinä huomioidaan myös Tukholman ohjelmaan (ja sitä koskevaan toimintasuunnitelmaan) sisältyvät ohjeet. Tukholman ohjelman luvussa 4.1 korostetaan tarvetta kehittää kattava sisäisen turvallisuuden strategia, jossa kunnioitetaan perusoikeuksia sekä kansainvälisen suojelun ja oikeusvaltion periaatetta. Tukholman ohjelman mukaan sisäisen turvallisuuden strategian kehittäminen, seuranta ja toteuttaminen pitäisi myös asettaa yhdeksi Euroopan unionin toiminnasta tehdyn sopimuksen 71 artiklan mukaisesti perustetun sisäisen turvallisuuden pysyvän komitean (COSI) päätehtävistä. Jotta sisäisen turvallisuuden strategiaa voitaisiin toteuttaa tehokkaasti, siihen pitäisi sisällyttää myös yhdennetyn rajavalvonnan turvallisuusnäkökohdat sekä tarvittaessa rikosoikeudellinen yhteistyö sisäistä turvallisuutta koskevan operatiivisen yhteistyön alalla. Tässä yhteydessä on myös tärkeää mainita, että Tukholman ohjelmassa kehotetaan omaksumaan sisäisen turvallisuuden strategiaa varten yhdennetty lähestymistapa, jossa huomioidaan myös EU:n ulkoisen turvallisuuden strategia sekä muut EU:n toimet erityisesti sisämarkkinoiden alalla.

Lausunnon tavoite

10. Tiedonannossa viitataan moniin politiikan aloihin, jotka Euroopan unionissa sisältyvät tai joilla on vaikutusta *sisäisen turvallisuuden* käsitteeseen laaja-alaisesti ymmärrettynä.

11. Lausunnon tavoitteena ei ole analysoida kaikkia tiedonannossa käsiteltyjä politiikan aloja ja yksittäisiä kysymyksiä, vaan tavoitteena on:

   — tarkastella tiedonannossa esitettyjä sisäisen turvallisuuden strategian tavoitteita yksityisyyden ja tietosuojan näkökulmasta sekä painottaa – samasta näkökulmasta – tarvetta liittää se muihin strategioihin, joita EU:ssa käsitellään ja hyväksytään;

   — määritellä tietyt tietosuojaa koskevat käsitteet, jotka olisi huomioitava suunniteltaessa, kehitettäessä ja toteutettaessa sisäisen turvallisuuden strategiaa EU:n tasolla;

   — antaa tarpeen mukaan ehdotuksia siitä, miten tietosuojaa koskevat seikat voitaisiin parhaiten huomioida toteutettaessa tiedonannossa ehdotettuja toimia.

12. Euroopan tietosuojavaltuutettu painottaa ehdotuksissaan etenkin sisäisen turvallisuuden strategian ja tiedonhallintastrategian välistä yhteyttä sekä kattavan tietosuojalainsäädännön luomista. Lisäksi Euroopan tietosuojavaltuutettu viittaa muun muassa seuraaviin käsitteisiin: paras käytettävissä oleva tekniikka ja ”sisäänrakennettu yksityisyyden suoja”, yksityisyyden suojaa ja tietosuojaa koskeva vaikutusten arviointi sekä rekisteröityjen oikeudet. Ne vaikuttavat välittömästi sisäisen turvallisuuden strategian suunnitteluun ja toteuttamiseen. Lausunnossa esitetään myös huomioita tietyistä erityisaloista, kuten yhdennetystä rajaturvallisuudesta, Euroopan rajavalvontajärjestelmästä (EUROSUR) ja henkilötietojen käsittelystä Euroopan rajaturvallisuusvirastossa (Frontex), sekä joistakin muista aloista, kuten verkkoympäristöstä ja terrorismin rahoituksen jäljittämisohjelmasta (TFTP).

II YLEISIÄ HUOMIOITA

Sisäisen turvallisuuden strategiaa koskevia EU:n strategioita varten tarvitaan kokonaisvaltaisempi, kattavampi ja ”strategisempi” lähestymistapa

13. EU:ssa keskustellaan tällä hetkellä lukuisista Lissabonin sopimukseen ja Tukholman ohjelmaan perustuvista EU:n strategioista, jotka vaikuttavat välittömästi tai välillisesti tietosuojaan. Sisäisen turvallisuuden strategia on niistä yksi, ja se liittyy läheisesti muihin strategioihin (joita on käsitelty hiljattain komission tiedonannoissa tai joita on tarkoitus käsitellä lähitulevaisuudessa). Esimerkkeinä mainittakoon EU:n tiedonhallintastrategia ja eurooppalainen tiedonvaihtomalli, EU:n perusoikeuskirjan toteuttamista koskeva strategia, kokonaisvaltainen tietosuojastrategia sekä EU:n terrorismin vastainen strategia. Euroopan tietosuojavaltuutettu kiinnittää lausunnossa erityistä huomiota tiedonhallintastrategiaan ja Euroopan unionin toiminnasta tehdyn sopimuksen 16 artiklaan perustuvaan kattavaan tietosuojalainsäädäntöön. Ne liittyvät selkeimmin sisäisen turvallisuuden strategiaan tietosuojan näkökulmasta.

14. Edellä mainitut strategiat muodostavat yhdessä monitahoisen toisiinsa liittyvien poliittisten suuntaviivojen, ohjelmien ja suunnitelmien ”tilkkutäkin”, minkä vuoksi EU:ssa tarvitaan kattavaa ja yhtenäistä lähestymistapaa.

15. Yleisemmin voidaan todeta, että jos tulevia toimia toteutettaessa sovelletaan *eri strategioiden yhdistämiseen* perustuvaa lähestymistapaa, se osoittaisi, että EU:lla on yhtenäinen näkemys *EU:n strategioista* ja että kyseiset strategiat ja niitä käsittelevät viimeaikaiset tiedonannot liittyvät läheisesti toisiinsa. Tämä johtuu siitä, että Tukholman ohjelma muodostaa niille kaikille yhteisen viitekohdan. Tällä tavoin luotaisiin myös myönteisiä synergiaetuja vapauden, turvallisuuden ja oikeuden alueeseen liittyvien toimien välille sekä vältettäisiin päällekkäiset toimet kyseisellä alalla. Mikä tärkeintä, tällainen lähestymistapa myös tehostaisi ja johdonmukaistaisi tietosuojasäännösten soveltamista toisiinsa liittyvien strategioiden yhteydessä.

16. Euroopan tietosuojavaltuutettu korostaa, että yksi sisäisen turvallisuuden strategian tukipilareista on tehokas tiedonhallinta Euroopan unionissa. Sen pitäisi perustua tarpeellisuuden ja suhteellisuuden periaatteisiin, jotta tietojen vaihtaminen olisi perusteltua.

17. Kuten Euroopan tietosuojavaltuutetun lausunnossa tiedonhallintaa käsittelevästä tiedonannosta ([8]) todetaan, Euroopan tietosuojavaltuutettu korostaa sitä, että uusia henkilötietojen tallennusta ja vaihtoa koskevia säädösehdotuksia pitäisi antaa vain, jos niiden tarpeellisuus voidaan osoittaa konkreettisesti ([9]). Tämän lakisääteisen vaatimuksen pitäisi edistää ennakoivaa politiikkaa sisäisen turvallisuuden strategian toteuttamisessa. Se, että sisäisen turvallisuuden strategia edellyttää kattavaa lähestymistapaa, johtaa väistämättä myös siihen, että kaikki sisäisen turvallisuuden alalla nykyisin käytössä olevat välineet on arvioitava ennen kuin ehdotetaan uusia.

18. Tähän liittyen Euroopan tietosuojavaltuutettu esittää myös, että olemassa olevien välineiden säännöllistä arviointia koskevia lausekkeita sovellettaisiin useammin. Tällainen lauseke sisältyi esimerkiksi tietojen säilyttämisestä annettuun direktiiviin, jota arvioidaan parhaillaan ([10]).

Tietosuoja sisäisen turvallisuuden strategian tavoitteena

19. Tiedonannossa viitataan henkilötietojen suojaan kohdassa *Yhteisiin arvoihin perustuva turvallisuuspolitiikka*. Siinä todetaan, että sisäisen turvallisuuden strategian toteuttamissuunnitelman ja sen täytäntöönpanovälineiden ja -toimien tulee perustua yhteisiin arvoihin, kuten oikeusvaltion periaatteeseen ja EU:n peruskirjassa vahvistettujen perusoikeuksien noudattamiseen. Tähän liittyen kyseisessä kohdassa todetaan: ”Silloin kun lainvalvontatoimia EU:ssa tehostetaan tietojenvaihdon avulla, on myös suojattava yksilöiden oikeus yksityisyyteen ja heidän perusoikeutensa henkilötietojen suojaan.”

20. Tämä on myönteinen toteamus. Sen ei kuitenkaan voida sellaisenaan katsoa ratkaisevan sisäisen turvallisuuden strategiaan liittyviä tietosuojakysymyksiä. Tiedonannossa ei käsitellä tietosuojaa tarkemmin ([11]), eikä siinä myöskään selitetä, miten yksityisyys ja tietosuoja taataan sisäisen turvallisuuden strategiaa koskevissa käytännön toimissa.

([8]) Euroopan tietosuojavaltuutetun 30. syyskuuta 2010 antama lausunto komission tiedonannosta Euroopan parlamentille ja neuvostolle ”Katsaus tiedonhallintaan vapauden, turvallisuuden ja oikeuden alalla”.

([9]) Kyse on lakisääteisestä vaatimuksesta; katso erityisesti Euroopan yhteisöjen tuomioistuimen 2. marraskuuta 2010 antama tuomio yhdistetyissä asioissa C-92/09 ja C-93/09. Euroopan tietosuojavaltuutettu on korostanut tätä lähestymistapaa eri yhteyksissä myös esimerkiksi seuraavissa vapauden, turvallisuuden ja oikeuden aluetta koskevista säädösehdotuksista antamissaan lausunnoissa: 19. lokakuuta 2005 annettu lausunto kolmesta Schengenin tietojärjestelmän toista sukupolvea (SIS II) koskevasta ehdotuksesta; 20. joulukuuta 2007 annettu lausunto ehdotuksesta neuvoston puitepäätökseksi matkustajarekisterin (PNR) käytöstä lainvalvontatarkoituksiin; 18. helmikuuta 2009 annettu lausunto ehdotuksesta asetukseksi Eurodac-järjestelmän perustamisesta sormenjälkien vertailua varten (kolmannen maan kansalaisen tai kansalaisuudettoman henkilön johonkin jäsenvaltioon jättämän kansainvälistä suojelua koskevan hakemuksen käsittelystä vastuussa olevan jäsenvaltion määrittämisperusteiden ja -menettelyjen vahvistamisesta) annetun asetuksen (EY) N:o […/…] tehokkaaksi soveltamiseksi; 18. helmikuuta 2009 annettu lausunto ehdotuksesta asetukseksi kolmannen maan kansalaisen tai kansalaisuudettoman henkilön johonkin jäsenvaltioon jättämän kansainvälistä suojelua koskevan hakemuksen käsittelystä vastuussa olevan jäsenvaltion määrittämisperusteiden ja -menettelyjen vahvistamisesta; 7. lokakuuta 2009 annettu lausunto ehdotuksista, jotka koskevat lainvalvontaviranomaisten pääsyä Eurodac-järjestelmään.

([10]) Euroopan parlamentin ja neuvoston 15 päivänä maaliskuuta 2006 antama direktiivi 2006/24/EY yleisesti saatavilla olevien sähköisten viestintäpalvelujen tai yleisten viestintäverkkojen yhteydessä tuotettavien tai käsiteltävien tietojen säilyttämisestä ja direktiivin 2002/58/EY muuttamisesta, (EUVL L 105, 13.4.2006, s. 54).

([11]) Tietosuoja mainitaan erityisesti vain kohdassa, jossa viitataan henkilötietojen käsittelyyn Frontexissa.

21. Euroopan tietosuojavaltuutettu katsoo, että *sisäisen turvallisuuden strategian toteuttamissuunnitelman* yhtenä tavoitteena pitäisi olla *suoja* laajemmin ymmärrettynä, jotta kansalaisten suojelu vallitsevilta uhkilta ja toisaalta heidän yksityisyytensä suojaaminen ja oikeutensa henkilötietojen suojaan olisivat varmasti *oikealla tavalla* tasapainossa keskenään. Toisin sanoen turvallisuus- ja yksityisyyskysymykset on otettava huomioon myös sisäisen turvallisuuden strategiaa kehitettäessä, kuten Tukholman ohjelmassa ja neuvoston päätelmissä esitetään.

22. Itse asiassa EU:n sisäisen turvallisuuden strategian tavoitteena pitäisi nimenomaan olla turvallisuuden varmistaminen siten, että yksityisyyttä ja tietosuojaa kunnioitetaan täysimääräisesti. Tämän pitäisi näkyä kaikissa toimissa, joita jäsenvaltiot ja EU:n toimielimet toteuttavat strategian yhteydessä.

23. Tässä yhteydessä Euroopan tietosuojavaltuutettu viittaa tiedonantoon KOM(2010) 609 kattavasta lähestymistavasta henkilötietojen suojaan Euroopan unionissa ([12]). Euroopan tietosuojavaltuutettu antaa siitä pian erillisen lausunnon mutta korostaa tässä, ettei sisäisen turvallisuuden strategian tehokas toteuttaminen ole mahdollista, jollei sitä täydentämään luoda kestävää tietosuojajärjestelmää keskinäisen luottamuksen ja tehokkuuden parantamiseksi.

III SISÄISEN TURVALLISUUDEN STRATEGIAN SUUNNITTELUUN JA TOTEUTTAMISEEN SOVELLETTAVIA KÄSITTEITÄ

24. On selvää, että jotkin sisäisen turvallisuuden strategian tavoitteisiin liittyvistä toimista voivat muodostaa uhan yksilöiden yksityisyydelle ja tietosuojalle. Uhkien torjumiseksi Euroopan tietosuojavaltuutettu haluaa kiinnittää erityistä huomiota sellaisiin käsitteisiin kuin ”sisäänrakennetun yksityisyyden suoja”, yksityisyyden suojaa ja tietosuojaa koskeva vaikutusten arviointi, rekisteröityjen oikeudet sekä paras käytettävissä oleva tekniikka. Kaikki mainitut käsitteet pitäisi huomioida sisäisen turvallisuuden strategiaa toteutettaessa, ja ne voivat myös osaltaan edistää yksityisyyden suojan ja tietosuojan kunnioittamista tätä alaa koskevassa politiikassa.

Sisäänrakennettu yksityisyyden suoja

25. Euroopan tietosuojavaltuutettu on korostanut useaan otteeseen ja useissa lausunnoissa sisäänrakennettua yksityisyyden suojaa (englanniksi ”Privacy by design” tai ”Privacy by default”). Käsite on yleistymässä sekä yksityisellä että julkisella sektorilla, minkä vuoksi sen on oltava keskeisessä asemassa myös EU:n sisäisen turvallisuuden alalla sekä poliisi- ja oikeusasioissa ([13]).

26. Tiedonannossa ei mainita tätä käsitettä. Euroopan tietosuojavaltuutetun mukaan tätä käsitettä pitäisi soveltaa kohdennetuissa toimissa, joita ehdotetaan ja toteutetaan sisäisen turvallisuuden strategian yhteydessä. Tämä pätee erityisesti tavoitteeseen 4, ”vahvistetaan turvallisuutta rajavalvonnan avulla”, jossa mainitaan selvästi uusien teknologioiden käytön lisääminen rajatarkastuksissa ja rajavalvonnassa.

Yksityisyyden suojaa ja tietosuojaa koskeva vaikutusten arviointi

27. Euroopan tietosuojavaltuutettu kannustaa komissiota pohtimaan – osana tiedonantoon perustuvan sisäisen turvallisuuden strategian tulevaa suunnittelua ja toteuttamista – mitä *yksityisyyden suojaa ja tietosuojaa koskevalla vaikutusten arvioinnilla* todella tarkoitetaan vapauden, turvallisuuden ja oikeuden alueella ja erityisesti sisäisen turvallisuuden strategiassa.

28. Tiedonannossa käsitellään uhkien ja riskien arviointia, mikä on hyvä asia. Tiedonannossa ei kuitenkaan – missään kohdassa – mainita yksityisyyden suojaa ja tietosuojaa koskevaa vaikutusten arviointia. Euroopan tietosuojavaltuutettu katsoo, että sisäisen turvallisuuden strategiasta annetun tiedonannon täytäntöönpano antaisi hyvän tilaisuuden kehittää yksityisyyden suojaa ja tietosuojaa koskevia vaikutusten arviointeja sisäisen turvallisuuden alalla. Euroopan tietosuojavaltuutettu panee merkille, ettei tätä käsitettä määritellä tarkemmin eikä sitä aseteta toimintapoliittiseksi vaatimukseksi sen enempää tiedonannossa kuin komission vaikutusten arviointeja koskevissa ohjeissakaan ([14]).

29. Euroopan tietosuojavaltuutettu suositteleekin, että tulevia välineitä toteutettaessa yksityisyyden suojaa ja tietosuojaa koskevat vaikutukset arvioidaan nykyistä tarkemmin ja tehokkaammin joko erillisenä arviointina tai osana yleistä perusoikeuksiin kohdistuvien vaikutusten arviointia. Vaikutusten arvioinnissa ei pitäisi tyytyä vain mainitsemaan yleisiä käsitteitä tai analysoimaan toimintapoliittisia vaihtoehtoja, kuten nykyisin tehdään, vaan sen yhteydessä pitäisi suositella yksittäisiä ja konkreettisia suojatoimenpiteitä.

30. Tätä varten pitäisi kehittää erityisiä indikaattoreita ja ominaisuuksia, joiden avulla varmistetaan, että kaikki yksityisyyden suojaan ja tietosuojaan mahdollisesti vaikuttavat ehdotukset, joita EU:n sisäisen turvallisuuden alalla annetaan, ovat suhteellisuuden, tarpeellisuuden ja käyttötarkoituksen rajoittamisen periaatteiden näkökulmasta tarkkaan harkittuja.

31. Lisäksi tässä yhteydessä voisi olla hyvä viitata RFID-tunnisteista annetun suosituksen ([15]) kohtaan 4, jossa komissio kehottaa jäsenvaltioita varmistamaan, että elinkeinoelämä määrittelee yhteistyössä asiaan liittyvien kansalaisyhteiskunnan sidosryhmien kanssa kehyksen yksityisyyden suojaa ja

([12]) Komission tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle kattavasta lähestymistavasta henkilötietojen suojaan Euroopan unionissa, KOM(2010) 609.

([13]) Euroopan tietosuojavaltuutettu suositteli Tukholman ohjelmaa koskevasta komission tiedonannosta antamassaan lausunnossa, että tietojärjestelmien rakentajille ja käyttäjille pitäisi asettaa velvoite hyödyntää järjestelmiä, joissa noudatetaan sisäänrakennetun yksityisyyden suojan periaatteita.

([14]) SEC(2009) 92, 15.1.2009.

([15]) C(2009) 3200 lopullinen, 12.5.2009.

tietosuojaa koskeville vaikutusten arvioinneille. Myös tietosuojavaltuutettujen kansainvälisessä konferenssissa marraskuussa 2009 hyväksytyssä Madridin julkilausumassa suositeltiin, että yksityisyyden suojan ja tietosuojan vaikutukset arvioidaan ennen kuin uusia henkilötietojen käsittelyyn liittyviä tietojärjestelmiä ja -tekniikoita otetaan käyttöön tai nykyisiin tehdään olennaisia muutoksia.

Rekisteröityjen oikeudet

32. Euroopan tietosuojavaltuutettu panee merkille, ettei tiedonannossa käsitellä erikseen rekisteröityjen oikeuksia – tärkeää aihetta, joka on olennainen osa tietosuojaa ja joka pitäisi siten huomioida sisäisen turvallisuuden strategian suunnittelussa. On ehdottomasti varmistettava, että kaikissa erilaisissa EU:n sisäiseen turvallisuuteen liittyvissä järjestelmissä ja välineissä taataan henkilötietojen käsittelyn osalta samat oikeudet kaikille kansalaisille.

33. Tiedonannossa mainitaan useita järjestelmiä, jotka sisältävät erityiset säännöt rekisteröityjen oikeuksille (jotka koskevat myös sellaisia henkilöryhmiä kuin uhreja, rikoksesta epäiltyjä sekä siirtolaisia). Järjestelmien ja välineiden välillä on kuitenkin suuria eroja, mille ei ole kunnollisia perusteita.

34. Näin ollen Euroopan tietosuojavaltuutettu kehottaa komissiota pohtimaan lähitulevaisuudessa tarkemmin rekisteröityjen oikeuksien yhtenäistämistä EU:ssa sisäisen turvallisuuden strategian ja tiedonhallintastrategian alalla.

35. Erityistä huomiota pitäisi kiinnittää oikeussuojamekanismeihin. Sisäisen turvallisuuden strategiassa pitäisi varmistaa, että rekisterinpitäjillä on käytössään helposti saavutettava, tehokas ja edullinen valitusmenettely, jos yksilön oikeuksia ei ole kunnioitettu täysimääräisesti.

Paras käytettävissä oleva tekniikka

36. Sisäisen turvallisuuden strategian toteuttaminen edellyttää luonnollisesti sellaista tietotekniikkainfrastruktuuria, joka tukee tiedonannossa ehdotettuja toimia. Paras käytettävissä oleva tekniikka voi auttaa löytämään oikeanlaisen tasapainon sisäisen turvallisuuden strategian tavoitteiden ja yksilön oikeuksien kunnioittamisen välille. Tässä yhteydessä Euroopan tietosuojavaltuutettu haluaisi toistaa aiemmissa lausunnoissaan antamansa suosituksen ([16]), jonka mukaan komission pitäisi yhdessä alan sidosryhmien kanssa määrittää ja edistää konkreettisia toimenpiteitä parhaan käytettävissä olevan tekniikan soveltamiseksi. Tämä tarkoittaa tietyn toiminnan ja siinä käytettävien tapojen tehokkainta ja edistyneintä astetta, jolla voidaan osoittaa olevan sellaiset tekniset ja käytännölliset ominaisuudet, jotka tuottavat tehokkaasti tuloksia ja ovat samalla yksityisyyden suojaa ja tietosuojaa koskevien EU-säännösten mukaisia. Tämä lähestymistapa on täysin yhdenmukainen aiemmin mainitun sisäänrakennetun yksityisyyden suojan periaatteen kanssa.

37. Parasta käytettävissä olevaa tekniikkaa koskevien viiteasiakirjojen pitäisi tarpeen ja mahdollisuuksien mukaan sisältää ohjeita sisäisen turvallisuuden strategiaan sisältyvien toimenpiteiden käytännön toteuttamista varten sekä parantaa sen oikeusvarmuutta. Näin voitaisiin edistää myös kyseisten toimenpiteiden yhdenmukaistamista jäsenvaltioissa. Lisäksi yksityisyyden suojaa ja turvallisuutta edistävän parhaan käytettävissä olevan tekniikan määrittäminen helpottaisi tietosuojaviranomaisten valvontatyötä, koska heillä olisi siten käytössään yksityisyyden suojan ja tietosuojan alalle soveltuvia teknisiä viitteitä, jotka myös rekisterinpitäjät ovat hyväksyneet.

38. Euroopan tietosuojavaltuutettu tuo myös esiin, miten tärkeää on yhtenäistää sisäisen turvallisuuden strategia seitsemännen tutkimuksen, teknologian kehittämisen ja demonstroinnin puiteohjelman sekä turvallisuutta ja vapauksien suojelua koskevan puiteohjelman yhteydessä toteutettujen toimien kanssa. Yhtenäinen näkemys parhaan käytettävissä olevan tekniikan määrittämisessä auttaa luomaan uutta tietoa ja uusia valmiuksia, joita vaaditaan, jotta kansalaisia voidaan suojella perusoikeuksia loukkaamatta.

39. Euroopan tietosuojavaltuutettu korostaa myös Euroopan verkko- ja tietoturvaviraston (ENISA) asemaa laadittaessa ohjeita ja arvioitaessa tietoturvamekanismeja, joiden avulla voidaan varmistaa tietoteknisten järjestelmien yhtenäisyys ja saatavuus. Virasto on keskeisessä asemassa myös parhaan käytettävissä olevan tekniikan edistämisessä. Tähän liittyen Euroopan tietosuojavaltuutettu panee tyytyväisenä merkille, että Euroopan verkko- ja tietoturvavirasto on keskeisenä toimijana kehittämässä valmiuksia torjua verkkohyökkäyksiä ja verkkorikollisuutta ([17]).

Eri toimijoiden ja niiden tehtävien määrittäminen

40. On määritettävä aiempaa tarkemmin, mitkä toimijat ovat mukana sisäisen turvallisuuden strategian rakenteessa tai vaikuttavat siihen. Tiedonannossa mainitaan lukuisia toimijoita ja sidosryhmiä, kuten kansalaiset, oikeuslaitos, EU:n erillisvirastot, kansalliset viranomaiset, poliisiviranomaiset

([16]) Euroopan tietosuojavaltuutetun heinäkuussa 2009 antama lausunto älykkäistä liikennejärjestelmistä ja Euroopan tietosuojavaltuutetun joulukuussa 2007 antama lausunto RFID-tunnisteita koskevasta tiedonannosta. Katso myös Euroopan tietosuojavaltuutetun vuosikertomus 2006, s. 48.

([17]) Euroopan tietosuojavaltuutetulla on tarkoitus antaa joulukuun 2010 aikana lausunto ENISAn säädöskehyksestä.

ja yritykset. Eri toimijoiden erityistehtävät ja toimivalta pitäisi määrittää tarkemmin kunkin sisäisen turvallisuuden strategian yhteydessä ehdotettavan toimenpiteen kohdalla.

IV ERITYISIÄ HUOMIOITA SISÄISEN TURVALLISUUDEN STRATEGIAAN LIITTYVISTÄ POLITIIKAN ALOISTA

Yhdennetty rajaturvallisuus

41. Tiedonannon mukaan EU:lla on Lissabonin sopimuksen voimaantulon myötä entistä paremmat mahdollisuudet hyödyntää matkustaja- ja tavaraliikennettä koskevien rajaturvallisuuspolitiikkojen välisiä synergiaetuja. Tiedonannossa todetaan, että ”henkilöiden liikkuvuuden alalla EU voi tarkastella muuttoliikkeen hallintaa ja rikollisuuden torjuntaa yhdennettyyn rajaturvallisuusstrategiaan kuuluvina rinnakkaisina tavoitteina”. Rajavalvonta nähdään tiedonannossa erinomaisena keinona torjua vakavaa kansainvälistä rikollisuutta ([18]).

42. Euroopan tietosuojavaltuutettu panee myös merkille, että tiedonannossa määritetään strategian kolme osa-aluetta: 1) uuden teknologian tehostettu käyttö rajatarkastuksissa (SIS II, viisumitietojärjestelmä VIS, maahantulo- ja maastapoistumisjärjestelmä sekä rekisteröityjen matkustajien asemaa koskeva ohjelma,) 2) uuden teknologian tehostettu käyttö rajavalvonnassa (Euroopan rajavalvontajärjestelmä EUROSUR), 3) jäsenvaltioiden toimien tehostettu koordinointi Frontexin johdolla.

43. Euroopan tietosuojavaltuutettu käyttää tilaisuuden hyväkseen ja palauttaa tässä lausunnossa mieliin useissa aiemmissa lausunnoissa esittämänsä kehotuksen: EU:lle pitäisi luoda selkeä rajaturvallisuuspolitiikka, jossa noudatetaan täysimääräisesti tietosuojasäännöksiä. Euroopan tietosuojavaltuutettu katsoo, että sisäisen turvallisuuden strategian ja tiedonhallinnan parissa tehtävä työ luo erittäin hyvän mahdollisuuden edetä noilla aloilla konkreettisemmin kohti johdonmukaista toimintapoliittista lähestymistapaa.

44. Euroopan tietosuojavaltuutettu panee merkille, että tiedonannossa viitataan lukuisiin laaja-alaisiin järjestelmiin, joista osa on jo käytössä ja osa otetaan mahdollisesti käyttöön lähitulevaisuudessa (esimerkiksi SIS, SIS II ja VIS). Tiedonannossa viitataan myös – samassa yhteydessä – järjestelmiin, joista komissio antaa mahdollisesti ehdotuksia myöhemmin mutta joista ei ole vielä päätetty (esimerkiksi rekisteröityjen matkustajien ohjelma ja maahantulo- ja maastapoistumisjärjestelmä). Tässä yhteydessä on muistettava, ettei kyseisten järjestelmien tavoitteita tai käyttöönoton perusteita ole vielä täsmennetty ja osoitettu esimerkiksi komission tekemien vaikutusten arviointien kautta. Jos näin ei tehdä, tiedonannon voidaan katsoa ennakoivan päätöksentekomenettelyä, eli siinä ei oteta huomioon, ettei rekisteröityjen matkustajien ohjelman eikä maahantulo- ja maastapoistumisjärjestelmän käyttöönotosta Euroopan unionissa ole vielä päätetty.

45. Näin ollen Euroopan tietosuojavaltuutettu ehdottaa, ettei sisäisen turvallisuuden strategian toteuttamisen suunnittelussa tehdä jatkossa vastaavia ennakointeja. Kuten edellä todettiin, uusien laaja-alaisten ja yksityisyyden suojaan vaikuttavien järjestelmien käyttöönotosta pitäisi päättää vasta sen jälkeen, kun kaikki nykyiset järjestelmät on arvioitu asianmukaisesti tarpeellisuuden ja suhteellisuuden näkökulmasta.

EUROSUR

46. Tiedonannon mukaan komissio antaa vuonna 2011 säädösehdotuksen EUROSUR-järjestelmän perustamisesta sisäisen turvallisuuden ja rikoksentorjunnan parantamiseksi. Tiedonannon mukaan EUROSURin yhteydessä hyödynnetään EU-rahoituksen avulla eri tutkimushankkeiden ja -toimien yhteydessä kehitettyä uutta teknologiaa, kuten satelliittikuvausjärjestelmiä, joiden avulla voidaan havaita ja jäljittää kohteita merirajoilla, esimerkiksi nopeita aluksia, joilla tuodaan huumeita EU:n alueelle.

47. Tähän liittyen Euroopan tietosuojavaltuutettu huomauttaa, ettei ole selvää, sisältyykö henkilötietojen käsittely EUROSUR-järjestelmässä säädösehdotukseen, jonka komissio aikoo antaa EUROSURista vuonna 2011, ja jos sisältyy, niin miten laajaa se olisi. Komission kanta tähän ei käy selvästi ilmi tiedonannosta. Asia on kuitenkin hyvin olennainen ottaen huomioon, että tiedonannossa EUROSUR ja Frontex liitetään selvästi toisiinsa taktisella, operatiivisella ja strategisella tasolla (katso Frontexia koskevat huomiot jäljempänä) sekä vaaditaan tiivistä yhteistyötä niiden välillä.

Henkilötietojen käsittely Frontexissa

48. Euroopan tietosuojavaltuutettu antoi 17. toukokuuta 2010 lausunnon Frontexin perustamisasetuksen muuttamisesta ([19]). Lausunnossa tietosuojavaltuutettu vaati, että henkilötietoja koskevista kysymyksistä keskustellaan kunnolla ja perinpohjaisesti, kun Frontexin nykyistä asemaa vahvistetaan ja sille annetaan uusia toimivaltuuksia.

49. Tiedonannossa viitataan tarpeeseen vahvistaa Frontexin asemaa ulkorajoilla tavoitteen 4, ”vahvistetaan turvallisuutta rajavalvonnan avulla”, yhteydessä. Tähän liittyen tiedonannossa todetaan, että saamiensa kokemusten perusteella ja EU:n yleisen tiedonhallintastrategian puitteissa komissio katsoo, että myöntämällä Frontexille valtuudet käsitellä ja käyttää näitä tietoja rajoitetusti ja henkilötietojen hallintaa

([18]) Lehdistötiedote ”EU:n sisäisen turvallisuuden strategian toteuttaminen: viisi askelta kohti turvallisempaa Eurooppaa”, memo 10/598.

([19]) Euroopan tietosuojavaltuutetun 17. toukokuuta 2010 antama lausunto ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi Euroopan unionin jäsenvaltioiden operatiivisesta ulkorajayhteistyöstä huolehtivan viraston (Frontex) perustamisesta annetun neuvoston asetuksen (EY) N:o 2007/2004 muuttamisesta.

koskevien selkeästi määriteltyjen sääntöjen mukaisesti voidaan merkittävällä tavalla edistää rikollisjärjestöjen hajottamista. Tämä lähestymistapa on uusi verrattuna komission ehdotukseen Frontexin perustamisasetuksen muuttamisesta. Euroopan parlamentti ja neuvosto käsittelevät ehdotusta parhaillaan, eikä siinä mainita mitenkään henkilötietojen käsittelyä.

50. Edellä mainitut seikat huomioon ottaen Euroopan tietosuojavaltuutettu paneekin tyytyväisenä merkille, että tiedonannossa viitataan tilanteisiin, joissa tietojen käsittely saattaisi olla tarpeen (esimerkiksi riskianalyysi, yhteisten operaatioiden parempi kohdentaminen tai tietojen vaihtaminen Europolin kanssa). Tiedonannossa todetaan, että rikollisia koskevia tietoja – joita Frontex saa haltuunsa operaatioidensa yhteydessä – ei voida nykyisin hyödyntää edelleen riskianalyysien laatimista tai tulevien yhteisten operaatioiden kohdentamista varten. Tärkeitä tietoja epäillyistä rikollisista ei voida myöskään luovuttaa toimivaltaisille kansallisille viranomaisille tai Europolille lisätutkimuksia varten.

51. Euroopan tietosuojavaltuutettu toteaa kuitenkin, ettei tiedonannossa viitata käynnissä olevaan keskusteluun Frontexin säädöskehyksen muuttamisesta. Keskustelussa pyritään löytämään lainsäädännöllisiä ratkaisuja, kuten edellä todetaan. Lisäksi tiedonannossa korostetaan Frontexin asemaa rikollisjärjestöjen hajottamisessa sanamuodoin, joiden voidaan tulkita tarkoittavan Frontexin toimivaltuuksien laajentamista. Euroopan tietosuojavaltuutettu ehdottaa, että tämä otetaan huomioon sekä Frontexin perustamisasetuksen muuttamisen että sisäisen turvallisuuden strategian toteuttamisen yhteydessä.

52. Euroopan tietosuojavaltuutettu kiinnittää huomiota myös tarpeeseen varmistaa, ettei Europolin ja Frontexin toiminnassa ole päällekkäisyyksiä. Tähän liittyen Euroopan tietosuojavaltuutettu panee tyytyväisenä merkille, että tiedonannon mukaan Frontexin ja Europolin tehtävien päällekkäisyys on vältettävä. Tätä asiaa pitäisi kuitenkin käsitellä perusteellisemmin sekä Frontexin perustamisasetuksen muuttamisen että sisäisen turvallisuuden strategian toteuttamistoimien yhteydessä, koska molemmissa pyritään tiivistämään Frontexin ja Europolin välistä yhteistyötä. Tämä on erityisen tärkeää käyttötarkoituksen rajoittamista ja tiedon laatua koskevien periaatteiden näkökulmasta. Sama huomio pätee tulevaan yhteistyöhön muiden virastojen, kuten Euroopan verkko- ja tietoturvaviraston (ENISA) tai Euroopan turvapaikka-asioiden tukiviraston, kanssa.

Biometristen tietojen käyttö

53. Tiedonannossa ei käsitellä erikseen sitä, että biometristen tietojen käyttö on lisääntymässä vapauden, turvallisuuden ja oikeuden alueella muun muassa EU:n laaja-alaisissa tietojärjestelmissä ja muissa rajaturvallisuuden välineissä.

54. Euroopan tietosuojavaltuutettu haluaakin tässä yhteydessä toistaa ehdotuksensa ([20]), jonka mukaan tämä tietosuojan näkökulmasta hyvin arkaluonteinen asia on otettava asianmukaisesti huomioon sisäisen turvallisuuden strategiaa toteutettaessa etenkin rajaturvallisuuden alalla.

55. Euroopan tietosuojavaltuutettu kehottaa myös kehittämään selkeän ja tiukan politiikan biometristen tietojen käyttöä varten vapauden, turvallisuuden ja oikeuden alueella. Politiikan pitäisi perustua siihen, että biometristen tietojen käytön tarpeellisuus arvioidaan perinpohjaisesti ja tapauskohtaisesti, ja siinä pitäisi noudattaa sellaisia tietosuojan perusperiaatteita kuin suhteellisuus, tarpeellisuus ja käyttötarkoituksen rajoittaminen.

Terrorismin rahoittamisen jäljittämisohjelma (TFTP)

56. Tiedonannon mukaan komissio kehittää vuoden 2011 aikana politiikan EU:ssa tapahtuvaa rahaliikenteen sanomavälitystietojen keräämistä ja analysointia varten. Tässä yhteydessä Euroopan tietosuojavaltuutettu viittaa 22. kesäkuuta 2010 antamaansa lausuntoon terrorismin rahoituksen jäljittämisohjelmaa (TFTP II) varten tapahtuvasta rahaliikenteen sanomanvälitystietojen käsittelystä ja siirtämisestä EU:sta Yhdysvaltoihin ([21]). Kyseisessä lausunnossa esitetyt kriittiset huomiot pätevät yhtä lailla suunnitelmiin luoda EU:ssa puitteet rahaliikenteen sanomavälitystietoja varten. Näin ollen ne pitäisi ottaa huomioon tätä asiaa koskevissa keskusteluissa. Erityisesti olisi kiinnitettävä huomiota suhteellisuuden periaatteeseen kerättäessä ja käsiteltäessä suuria määriä sellaisten henkilöiden tietoja, joita ei epäillä rikoksesta, sekä riippumattomien viranomaisten ja oikeuslaitosten harjoittaman valvonnan tehokkuuteen.

Kansalaisten ja yritysten turvallisuus verkkoympäristössä

57. Euroopan tietosuojavaltuutettu on tyytyväinen siihen, että tiedonannossa painotetaan ennaltaehkäiseviä toimia EU:ssa. Hän katsoo myös, että tietoteknisten verkkojen turvallisuuden parantaminen on keskeinen tekijä toimivan tietoyhteiskunnan luomisessa. Euroopan tietosuojavaltuutettu tukee myös erityistoimia, joilla voidaan parantaa valmiuksia reagoida verkkohyökkäyksiä vastaan, kehittää lainvalvontaelinten ja oikeuslaitosten valmiuksia ja luoda kumppanuuksia teollisuuden kanssa kansalaisten ja yritysten mukaan ottamiseksi. ENISAn tuki monissa tätä tavoitetta koskevissa toimissa on myös myönteinen asia.

([20]) Katso erityisesti alaviitteessä 8 mainittu Euroopan tietosuojavaltuutetun lausunto, joka koskee tiedonantoa katsauksesta tiedonhallintaan vapauden, turvallisuuden ja oikeuden alueella.

([21]) Euroopan tietosuojavaltuutetun 22. kesäkuuta 2010 antama lausunto ehdotuksesta neuvoston päätökseksi terrorismin rahoituksen jäljittämisohjelmaa (TFTP II) varten tapahtuvaa rahaliikenteen sanomanvälitystietojen käsittelyä ja siirtämistä Euroopan unionista Yhdysvaltoihin koskevan Euroopan unionin ja Amerikan yhdysvaltojen välisen sopimuksen tekemisestä.

58. *Sisäisen turvallisuuden strategian toteuttamissuunnitelmassa* ei kuitenkaan käsitellä tarkemmin verkkoympäristöön kohdistuvia lainvalvontatoimia eikä sitä, miten kyseiset toimet saattavat vaarantaa yksilön oikeudet tai millaisia suojatoimenpiteitä tarvitaan. Euroopan tietosuojavaltuutettu kehottaa omaksumaan kunnianhimoisemman lähestymistavan asianmukaisiin takuisiin. Sen tavoitteena olisi suojella kaikkien yksilöiden perusoikeuksia – mukaan lukien henkilöt, joihin rikosten estämiseksi toteutettavat toimet mahdollisesti kohdistuvat.

V **PÄÄTELMÄT JA SUOSITUKSET**

59. Euroopan tietosuojavaltuutettu kehottaa huomioimaan sisäisen turvallisuuden strategian toteuttamisessa erilaiset EU:n strategiat ja tiedonannot. Tämän lähestymistavan pohjalta pitäisi laatia konkreettinen toimintasuunnitelma, jonka yhteydessä myös arvioidaan tarpeet asianmukaisesti. Sen seurauksena EU:lle pitäisi muodostua sisäisen turvallisuuden strategian alalla kattava, yhdennetty ja hyvin jäsennelty politiikka.

60. Euroopan tietosuojavaltuutettu haluaa tässä yhteydessä korostaa myös lakisääteistä vaatimusta, jonka mukaan kaikki sisäisen turvallisuuden strategian ja tietojenvaihdon alalla nykyisin sovellettavat välineet on arvioitava kunnolla ennen uusien ehdottamista. Näin ollen on erittäin suositeltavaa hyväksyä säännöksiä, joissa säädetään keskeisten välineiden tehokkuuden säännöllisestä arvioimisesta.

61. Euroopan tietosuojavaltuutettu ehdottaa, että neuvoston marraskuun 2010 päätelmissä esitettyä monivuotista strategiaohjelmaa laadittaessa huomioidaan jatkuva työ, jota tehdään Euroopan unionin toiminnasta tehdyn sopimuksen 16 artiklaan perustuvan kattavan tietosuojalainsäädännön alalla. Erityisesti mainittakoon komission tiedonanto KOM(2010) 609.

62. Euroopan tietosuojavaltuutettu tekee useita ehdotuksia tietosuojan alalla keskeisistä käsitteistä, jotka pitäisi ottaa huomioon sisäisen turvallisuuden strategiassa. Niitä ovat esimerkiksi sisäänrakennettu yksityisyyden suoja, yksityisyyden suojaa ja tietosuojaa koskeva vaikutusten arviointi sekä paras käytettävissä oleva tekniikka.

63. Euroopan tietosuojavaltuutettu suosittelee, että tulevia välineitä toteutettaessa arvioidaan yksityisyyden suojaa ja tietosuojaa koskevat vaikutukset joko erillisenä arviointina tai osana yleistä perusoikeuksiin kohdistuvien vaikutusten arviointia.

64. Euroopan tietosuojavaltuutettu kehottaa myös komissiota laatimaan sisäisen turvallisuuden strategian yhteydessä johdonmukaiset ja yhtenäiset toimintapoliittiset ohjeet biometristen tietojen käytön edellytyksille sekä yhtenäistämään rekisteröityjen oikeuksia EU:n tasolla.

65. Euroopan tietosuojavaltuutettu esittää myös useita huomioita henkilötietojen käsittelystä rajaturvallisuuden alalla erityisesti Frontexissa ja mahdollisesti EUROSUR-järjestelmässä.

Tehty Brysselissä 17 päivänä joulukuuta 2010.

Peter HUSTINX

Euroopan tietosuojavaltuutettu