

MDY Partanen Aleksandra

21.05.2007

Eduskunta
Suuri valiokunta

Viite

KOM(2007) 228 lopullinen

Asia

Komission tiedonanto Euroopan parlamentille ja neuvostolle tietosuojan vahvistamisesta yksityisyyden suojaa parantavilla tekniikoilla.

U/E-tunnus:

EUTORI-numero:

EU/2007/0998

Ohessa lähetetään perustuslain 97§:n mukaisesti selvitys eduskunnan suurelle valiokunnalle asiakohdassa mainitusta Euroopan komission tiedonannosta, sekä tiedonannon suomen- ja ruotsinkieliset versiot.

Ylijohtaja, osastopäällikkö

Liisa Ero

LIITTEET LVM2007-00188, KOM(2007) 228 lopullinen, KOM(2007) 228 slutlig

Asiasanat	tietosuoja
Hoitaa	LVM, OM, VM
Tiedoksi	EUE, KTM, MMM, OPM, PLM, SM, STM, TH, TM, UM, VNEUS

VLV Nordenstreng Laura

21.05.2007

Asia

Komission tiedonanto Euroopan parlamentille ja neuvostolle tietosuojan vahvistamisesta yksityisyyden suojaa parantavilla tekniikoilla.

Kokous

Liitteet

Viite

KOM(2007) 228 lopullinen

EUTORI/Eurodoc nro:

EU/2007/0998

U-tunnus / E-tunnus:

-

Käsittelyn tarkoitus ja käsittelyvaihe:

-

Asiakirjat:

Komission asiakirja KOM(2007) 228 lopullinen: *Komission tiedonanto Euroopan parlamentille ja neuvostolle tietosuojan vahvistamisesta yksityisyyden suojaa parantavilla tekniikoilla.*

EU:n oikeuden mukainen oikeusperusta/päätöksentekomenettely:

-

Käsittelijä(t):

Liikenne- ja viestintäministeriö, neuvotteleva virkamies Laura Nordenstreng, puh. 160 28609, laura.nordenstreng@mintc.fi

Liikenne- ja viestintäministeriö, viestintäneuvos, yksikön päällikkö, Juhapekka Ristola, puh. 160 28348, juhapekka.ristola@mintc.fi

Suomen kanta/ohje:

-

Pääasiallinen sisältö:

Komissio antoi 2.5.2007 tiedonannon tietosuojan vahvistamisesta yksityisyyden suojaa parantavilla tekniikoilla. Tiedonanto on jatkoa komission 15.5.2003 antamalle ensimmäiselle kertomukselle tietosuojadirektiivin täytäntöönpanosta (KOM(2003) 265 lopullinen).

Yksityisyyden suojaa parantavilla tekniikoilla tarkoitetaan tiedonannossa yhtenäistä tieto- ja viestintätekniisten toimenpiteiden järjestelmää, jolla suojataan yksityisyyttä poistamalla henkilötiedot kokonaan tai osittain tai ehkäisemällä tarpeeton ja/tai epätoivottu henkilötietojen käsittely heikentämättä kuitenkaan tietojärjestelmän toimivuutta. Kysymyksessä on siis tekninen tapa vahvistaa tietojärjestelmien tietosuojaa. Yksityisyyden suojaa parantavien tekniikoiden käytöllä voidaan tukea sellaisten tieto- ja viestintäjärjestelmien ja -palveluiden suunnittelua, joissa henkilötietojen keruu ja käyttö on rajattu minimiin ja joilla voidaan helpottaa tietosuojasääntöjen noudattamista.

Tiedonannossa komissio katsoo, että yksityisyyden suojaa parantavia tekniikoita olisi kehitettävä edelleen ja ne olisi otettava laajemmin käyttöön erityisesti silloin, kun on kyse henkilötietojen käsittelystä tieto- ja viestintäverkoissa. Komission näkemyksen mukaan kyseisten tekniikoiden laajempi käyttö parantaisi yksityisyyden suojaa ja helpottaisi tietosuojasääntöjen noudattamista. Kyseisten tekniikoiden käytöllä täydennettäisiin nykyistä tietosuojaa koskevaa oikeudellista kehystä ja nykyisiä lainvalvontakeinoja. Se, että tietojen käsittelyyn osallistuu monia eri toimijoita, ja tietojen käsittely tapahtuu monen eri maan lainkäyttöalueella, voi vaikeuttaa oikeudellisen kehyksen soveltamisen valvontaa. Yksityisyyden suojaa parantavien tekniikoiden avulla voitaisiin välttää tietyt tietosuojasääntöjen rikkomiset, koska säännösten rikkominen muuttuisi niiden ansiosta teknisesti vaikeammaksi. Tekniikoiden käyttö ei kuitenkaan tarkoittaisi, että toimijat voitaisiin vapauttaa lakisääteisistä velvoitteistaan, vaan tekniikoiden käytössä olisi noudatettava voimassa olevia tietosuojasäännöksiä.

Tiedonannossa esitellään erilaisia toimenpiteitä, joihin komissio aikoo ryhtyä tukeakseen yksityisyyden suojaa parantavien tekniikoiden kehittämistä ja käyttöä. Toimenpiteissä on mukana useita eri toimijoita kuten komission omat yksiköt, kansalliset viranomaiset, elinkeinoelämän edustajat sekä kuluttajat. Kaikkien toimenpiteiden toteuttamisessa komissio tulee kiinnittämään erityistä huomiota pienten ja keskisuurten yritysten erityistilanteeseen sekä siihen, millaisia mahdollisuuksia niillä olisi käyttää kyseisiä tekniikoita.

Komission toimenpiteet on jaettu kolmen alatavoitteen alle. Ensimmäisessä alatavoitteessa pyritään yksityisyyden suojaa parantavien tekniikoiden kehittämisen tukemiseen. Tavoitteen toteuttaminen edellyttää sekä tekniikoihin liittyvien tarpeiden ja teknisten vaatimusten kartoittamista että myös konkreettisia toimia tekniikoihin liittyvien lopputuotteiden kehittämiseksi. Tässä työssä sidosryhmillä on keskeinen rooli. Keskeisiä sidosryhmiä ovat muun muassa tieto- ja viestintätekniikan alan edustajat, yksityisyyden suojaa parantavien tekniikoiden kehittäjät, tietosuoja- ja lainvalvontaviranomaiset sekä kuluttajat ja kansalaisjärjestöt.

Toisessa alatavoitteessa pyrkimyksenä on yksityisyyden suojaa parantavien tekniikoiden käytön lisääminen rekisterinpitäjien keskuudessa. Rekisterinpitäjillä tulee olemaan tämän tavoitteen toteuttamisessa keskeinen rooli, mutta myös komissio tulee muun muassa omilla tutkimustoimenpiteillään edesauttamaan tavoitteen toteuttamista. Komissio aikoo myös selvittää, onko tarpeen laatia standardeja henkilötietojen luvalliselle käytölle

yksityisyyden suojaa parantavilla tekniikoilla. Standardoinnin ohella kyseeseen voisi myös tulla tietojenkäsittelyyn liittyviä tietoturvatoinenpiteitä koskevien kansallisten teknisten sääntöjen yhteensovittaminen lähinnä tietosuojadirektiivin 29 artiklan mukaisen tietosuojatyöryhmän ja kansallisten tietosuojaviranomaisten toimenpitein.

Kolmannessa alatavoitteessa tavoitteena on kuluttajien kannustaminen käyttämään yksityisyyttä parantavia tekniikoita. Tavoitteen saavuttaminen edellyttää sekä kuluttajien tietoisuuden lisäämistä että myös kuluttajien avustamista tietoon perustuvien valintojen tekemisessä. Viimeksi mainittuun liittyen komissio aikoo tutkia mahdollisuutta ottaa käyttöön EU:n laajuinen yksityisyyden suojaa koskevien tunnusten järjestelmä, joka voisi helpottaa yksityisyyden suojaa parantavia tekniikoita käyttävien tuotteiden ja palvelujen tunnistamista. Tutkimustyössään komissio tulee myös arvioimaan tällaisen järjestelmän taloudellisia ja yhteiskunnallisia vaikutuksia.

Kansallinen käsittely:

-

Eduskuntakäsittely:

-

Käsittely Euroopan parlamentissa:

-

Kansallinen lainsäädäntö, ml. Ahvenanmaan asema:

-

Taloudelliset vaikutukset:

-

Muut mahdolliset asiaan vaikuttavat tekijät:

-

Asiasanat
Hoitaa

Tiedoksi

FI

FI

FI



EUROOPAN YHTEISÖJEN KOMISSIO

Bryssel 2.5.2007
KOM(2007) 228 lopullinen

KOMISSION TIEDONANTO EUROOPAN PARLAMENTILLE JA NEUVOSTOLLE

tietosuojan vahvistamisesta yksityisyyden suojaa parantavilla tekniikoilla

KOMISSIION TIEDONANTO EUROOPAN PARLAMENTILLE JA NEUVOSTOLLE

tietosuojan vahvistamisesta yksityisyyden suojaa parantavilla tekniikoilla

(ETA:n kannalta merkityksellinen teksti)

1. JOHDANTO

Tieto- ja viestintätekniikan jatkuva intensiivinen kehitys on johtanut siihen, että tarjolla on alati uusia palveluja, jotka parantavat ihmisten elämää. Verkkoavaruudessa tapahtuva kanssakäyminen perustuu paljolti niiden ihmisten henkilötietoihin, jotka ostavat sieltä tavaroita ja palveluita, luovat yhteyksiä tai pitävät yhteyttä toisiinsa taikka julkistavat ajatuksiaan verkkosivuilla. Tästä kehityksestä saatavien etujen lisäksi se tuo tullessaan myös uusia riskejä, kuten väärän henkilöllisyyden käyttö, syrjivä profilointi, jatkuva seuranta tai petokset.

Euroopan unionin perusoikeuskirjan 8 artiklaan on kirjattu oikeus henkilötietojen suojaan. Tämä perusoikeus vahvistetaan henkilötietojen suojaa koskevassa yhteisön lainsäädännössä, joka sisältää erityisesti tietosuojadirektiivin 95/46/EY¹, sähköisen viestinnän tietosuojadirektiivin 2002/58/EY² ja tietosuoja-asetuksen (EY) N:o 45/2001³, joka kattaa henkilötietojen käsittelyn yhteisön toimielimissä ja elimissä. Tämä lainsäädäntö sisältää useita aineellisia säännöksiä, joilla asetetaan velvoitteita rekisterinpitäjille ja tunnustetaan rekisteröidyn oikeudet. Siinä säädetään myös säännösten rikkomisesta määrättävistä seuraamuksista ja tarkoituksenmukaisista korjaustoimenpiteistä sekä säännösten tehokkaan soveltamisen takaavien valvontajärjestelyiden käyttöönotosta.

Tämä järjestelmä voi kuitenkin osoittautua riittämättömäksi, kun henkilötietoja levitetään maailmanlaajuisesti tieto- ja viestintäverkoissa ja kun tietojen käsittelyssä on mukana lukuisia lainkäyttöalueita, jotka sijaitsevat usein EU:n ulkopuolella. Tällaisissa tilanteissa nykyiset säännöt saattavat osoittautua käyttökelpoisiksi ja niiden perusteella voidaan kartoittaa selkeät oikeudelliset ratkaisut. Lisäksi ne saattavat mahdollistaa niiden soveltamista valvovan toimivaltaisen viranomaisen yksilöinnin. Käytössä olevaan tekniikkaan liittyvien vaikeuksien tuloksena voi kuitenkin ilmetä huomattavia käytännön ongelmia, sillä tietojen käsittelyyn osallistuu eri paikoissa toimivia henkilöitä ja kansallisella tasolla annettujen hallinnollisten ja oikeudellisten päätösten noudattamisen valvonta muilla lainkäyttöalueilla, erityisesti EU:n ulkopuolisissa maissa, on usein ongelmallista.

¹ Euroopan parlamentin ja neuvoston direktiivi 95/46/EY, annettu 24 päivänä lokakuuta 1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta, EYVL L 281, 23.11.1995, s. 31.

² Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY, annettu 12 päivänä heinäkuuta 2002, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (sähköisen viestinnän tietosuojadirektiivi), EYVL L 201, 31.7.2002, s. 37.

³ Euroopan parlamentin ja neuvoston asetetus (EY) N:o 45/2001, annettu 18 päivänä joulukuuta 2000, yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta, EYVL L 8, 12.1.2001, s. 1–22.

Vaikka oikeudellinen vastuu tietosuojasääntöjen noudattamisesta kuuluu varsinaisesti rekisterinpitäjille, ne jakavat tietosuojanäkökohtiin liittyvän yhteiskunnallisen ja eettisen vastuun tietyiltä osin muiden tahojen kanssa. Näitä tahoja ovat muun muassa teknisten eritelmien laatijat ja sovellusten tai käyttöjärjestelmien varsinaiset valmistajat tai kehittäjät.

Tietosuojadirektiivin 17 artiklassa rekisterinpitäjä veloitetaan toteuttamaan tarpeelliset tekniset ja organisatoriset toimenpiteet sellaisen turvallisuustason varmistamiseksi, joka on riittävä suhteessa tietojen luonteeseen ja niiden käsittelyyn liittyviin riskeihin. Sähköisen viestinnän tietosuojadirektiivissä⁴ otetaan jo jossain määrin huomioon mahdollisuus lainsäädännön ja erityisesti tietosuojasääntöjen noudattamisen varmistamiseen tekniikan käytön avulla.

Lainsäädännössä on asetettu tavoitteeksi henkilötietojen käsittelyn rajaaminen minimiin ja nimettömän tai salanimellä julkaistun tiedon käyttö aina kun se on mahdollista. Tämän tavoitteen saavuttamista voitaisiin edistää yksityisyyden suojaa parantavilla tekniikoilla (*Privacy Enhancing Technologies*), joiden avulla päästäisiin helpommin tilanteeseen, jossa tietosuojasääntöjen ja yksilön oikeuksien rikkomista ei katsota pelkästään kielletyksi teoksi, josta määrätään seuraamuksia, vaan jossa sääntöjen ja oikeuksien rikkominen olisi lisäksi teknisesti nykyistä vaikeampaa.

Tämä tiedonanto annetaan tietosuojadirektiivin täytäntöönpanosta annetun ensimmäisen kertomuksen⁵ jatkoksi. Tiedonannossa luodaan katsaus yksityisyyden suojaa parantavista tekniikoista saatavaan hyötyyn, määritetään komission tavoitteet tietosuojan alalla näiden tekniikoiden käytön lisäämiseksi ja esitellään yksityiskohtaisesti toimia, jotka olisi toteutettava tämän tavoitteen saavuttamiseksi tukemalla yksityisyyden suojaa parantavien tekniikoiden kehittämistä ja niiden käyttöä rekisterinpitäjien ja kuluttajien tasolla.

2. MITÄ YKSITYISYYDEN SUOJAA PARANTAVAT TEKNIIKAT OVAT?

Yksityisyyden suojaa parantavista tekniikoista on laadittu useita määritelmiä, jotka ovat käytössä korkeakouluissa ja alan pilottihankkeissa. Esimerkiksi yhteisön rahoitusta saavassa PISA-hankkeessa näillä tekniikoilla tarkoitetaan yhtenäistä tieto- ja viestintätekniisten toimenpiteiden järjestelmää, jolla suojataan yksityisyyttä poistamalla henkilötiedot kokonaan tai osittain tai ehkäisemällä tarpeeton ja/tai epätoivottu henkilötietojen käsittely heikentämättä kuitenkaan tietojärjestelmän toimivuutta. Yksityisyyden suojaa parantavien tekniikoiden käytöllä voidaan tukea sellaisten tieto- ja viestintäjärjestelmien sekä -palveluiden suunnittelua, joissa henkilötietojen keruu ja käyttö on rajattu minimiin ja joilla helpotetaan tietosuojasääntöjen noudattamista. Komissio toteaa tietosuojadirektiivin täytäntöönpanosta annetussa ensimmäisessä kertomuksessa, että "...asianmukaiset tekniset toimenpiteet täydentävät olennaisesti oikeudellisia keinoja, ja niiden olisi kuuluttava kiinteänä osana kaikkiin toimiin, joiden tavoitteena on saavuttaa riittävä yksityisyyden suojan taso". Yksityisyyden suojaa parantavien tekniikoiden käytön odotetaan vaikeuttavan tiettyjen tietosuojasääntöjen rikkomista ja/tai helpottavan sääntörikkomusten havaitsemista.

Alati muuttuvassa tieto- ja viestintäteknisessä ympäristössä yksityisyyden suojan ja tietyiltä osin myös tietosuojalainsäädännön noudattamisen varmistavien tekniikoiden tehokkuus vaihtelee ja muuttuu ajan mittaan. Tekniikoita on lisäksi useita eri tyyppisiä. Ne voivat olla erillisiä työkaluja, joiden käyttö edellyttää kuluttajien panosta (kuluttajien on hankittava ne ja asennettava ne

⁴ Direktiivin 2002/58/EY johdanto-osan 46 kappale ja 14 artiklan 3 kohta.

⁵ KOM(2003) 265(01), 15.5.2003, ks.
http://eurlex.europa.eu/LexUriServ/site/en/com/2003/com2003_0265en01.pdf.

tietokoneisiinsa), tai ne voivat muodostaa varsinaisen tietojärjestelmärakenteen kiinteän osan. Seuraavassa mainitaan esimerkkejä yksityisyyden suojaa parantavista tekniikoista:

- Henkilötietojen automaattinen poistuminen tietyn ajan kuluttua tukee periaatetta, jonka mukaan käsiteltävien tietojen olisi oltava sellaisessa muodossa, josta rekisteröity on tunnistettavissa ainoastaan sen ajan kuin on tarpeen niiden tarkoitusten toteuttamista varten, joita varten tiedot kerättiin.
- Salausohjelmat, jotka estävät tiedon sieppaamisen Internetissä tapahtuvassa tiedonsiirrossa, auttavat rekisterinpitäjää täyttämään velvollisuutensa, jonka mukaan sen on toteutettava aiheelliset toimenpiteet henkilötietojen suojaamiseksi laittomalta käsittelyltä.
- Suodatinohjelmat, jotka estävät nk. evästeiden (*cookies*) tallentumisen käyttäjän tietokoneelle. Evästeet saavat tietokoneen tottelemaan joitakin ohjauskäskyjä ilman että käyttäjä on tietoinen siitä. Näillä ohjelmilla edistetään tietojen tasapuolisen ja lainmukaisen käsittelyn periaatteen noudattamista ja periaatetta, jonka mukaan henkilön on oltava tietoinen tietojensa käsittelystä.
- *Platform for Privacy Preferences (P3P)* -tekniikan avulla Internetin käyttäjät voivat arvioida, millaisia yksityisyyden suojaa koskevia periaatteita eri verkkosivustot noudattavat, ja verrata niitä omiin näkemyksiinsä siitä, millaisia tietoja he ovat valmiit luovuttamaan. P3P-tekniikan avulla rekisteröity voi varmistaa antaneensa tietoon perustuvan suostumuksen itseään koskevien tietojen käsittelyyn.

3. KOMISSIO TUKEE YKSITYISYYDEN SUOJAA PARANTAVIEN TEKNIIKOIDEN KÄYTTÖÄ

Komissio katsoo, että yksityisyyden suojaa parantavia tekniikoita olisi kehitettävä edelleen ja ne olisi otettava laajemmin käyttöön erityisesti silloin, kun on kyse henkilötietojen käsittelystä tieto- ja viestintäverkoissa. Komission näkemyksen mukaan kyseisten tekniikoiden laajempi käyttö parantaisi yksityisyyden suojaa ja helpottaisi tietosuojasääntöjen noudattamista. Lisäksi kyseisten tekniikoiden käytöllä täydennettäisiin nykyistä oikeudellista kehystä ja nykyisiä lainvalvontakeinoja.

Turvallisen tietoyhteiskunnan strategiaa koskevassa tiedonannossaan (KOM(2006) 251, 31.5.2006) komissio kehotti erityisesti yksityistä sektoria lisäämään ”tietoturvaa tehostavien tuotteiden, prosessien ja palvelujen käyttöönottoa käyttäjätunnusvarkauksien ja muiden yksityisyyttä loukkaavien hyökkäysten ehkäisemiseksi ja torjumiseksi”. Lisäksi yleiseurooppalaisen EIDM-puitteiden käyttöönotosta vuoteen 2010 mennessä annetun komission suunnitelman⁶ mukaan yksi sähköisen identiteetin hallinnan pääperiaatteista on, että ”järjestelmän on oltava turvallinen, siinä on oltava käyttäjän yksityisyyden suojaamisen kannalta välttämättömät suojakeinot ja sen käyttö on voitava mukauttaa paikallisiin etunäkökohtiin ja salassapitopainotuksiin”.

Se, että tietojen käsittelyyn osallistuu monia eri toimijoita ja se tapahtuu monen eri maan lainkäyttöalueella, voi vaikeuttaa oikeudellisen kehyksen soveltamisen valvontaa. Yksityisyyden suojaa parantavien tekniikoiden käytön avulla voitaisiin toisaalta välttää tietyt tietosuojasääntöjen rikkomiset, joiden seurauksena rikotaan myös perusoikeuksia, kuten oikeutta yksityisyyteen, sillä rikkominen muuttuisi niiden ansiosta teknisesti vaikeammaksi. Komissio on tietoinen siitä, että vaikka tekniikka on keskeisessä asemassa yksityisyyden suojaamisessa, se ei yksistään takaa

⁶ http://ec.europa.eu/information_society/activities/egovernment_research/doc/eidm_roadmap_paper.pdf.

riittävää suojaa. Yksityisyyden suojaa parantavien tekniikoiden käytössä on noudatettava täytäntöönpanokelpoisia tietosuojasääntöjä, joilla kaikille tarjotaan tietystä määrin erikseen sovittavissa oleva yksityisyyden suojan taso. Näiden tekniikoiden käyttö ei kuitenkaan tarkoita sitä, että toimijat voitaisiin vapauttaa tietyistä lakisääteisistä velvoitteistaan (esim. velvoitteesta, jonka mukaan toimijoiden on myönnettävä käyttäjille oikeus tutustua heitä koskeviin tietoihin).

Myös tärkeät yleistä etua koskevat näkökohdat voitaisiin ottaa nykyistä paremmin huomioon. Tietosuojaa koskevan lainsäädännön mukaan yleisten periaatteiden noudattamista ja yksilöiden oikeuksien kunnioittamista voidaan rajoittaa tärkeisiin yleisiin etunäkökohtiin kuten yleiseen turvallisuuteen, rikosten torjuntaan tai kansanterveyteen liittyvistä syistä. Näihin rajoituksiin sovellettavista ehdoista säädetään tietosuojadirektiivin 13 artiklassa ja sähköisen viestinnän tietosuojadirektiivin 15 artiklassa. Kyseiset ehdot vastaavat sisällöltään Euroopan ihmisoikeussopimuksen 8 artiklaa, jonka mukaan yksityisyyteen puuttuminen voi olla perusteltua silloin, kun laki sen sallii ja se on demokraattisessa yhteiskunnassa välttämätöntä oikeasuhteista ja välttämätöntä perusteltua julkista tarkoitusta varten.⁷ Yksityisyyden suojaa parantavien tekniikoiden käyttö ei saisi estää lainvalvontaviranomaisia eikä muita toimivaltaisia viranomaisia hoitamasta tärkeää yleistä etua koskevan syyn vuoksi lakisääteisiä tehtäviään, kuten tietoverkkorikollisuuden tai terrorismin torjunta tai tarttuvien tautien leviämisen ehkäiseminen. Vastuuviranomaisten olisi saatava tarvittaessa käyttöönsä henkilötietoja kyseisten tehtävien hoitamiseksi lakisääteisten menettelyiden, ehtojen ja suojakeinojen mukaisesti.

Tietosuojasääntöjen parempi noudattaminen vaikuttaisi myönteisesti myös kuluttajien luottamukseen erityisesti verkkoavaruutta kohtaan. Monet lupaavat lisäarvopalvelut, jotka perustuvat henkilötietojen siirtoon tietoverkoissa ja joita ovat esimerkiksi verkko-oppiminen, sähköiset viranomaispalvelut, sähköiset terveydenhuolto- ja pankkipalvelut, verkkokauppa ja nk. älyautojärjestelmät. Kuluttajat voisivat olla varmoja siitä, että tunnistautumista, palveluiden vastaanottamista tai maksujen suorittamista varten luovutettuja tietoja käytetään ainoastaan laillisiin tarkoituksiin ja että digitaaliympäristössä toimiminen ei tapahdu heidän oikeuksiensa kustannuksella.

4. TÄHÄNASTINEN TOIMINTA JA JATKOTOIMET

Parantaakseen yksityisyyden suojan ja tietosuojan tasoa yhteisössä muun muassa tukemalla yksityisyyden suojaa parantavien tekniikoiden kehittämistä ja käyttöä komissio aikoo harjoittaa jäljempänä kuvailtua toimintaa, jossa on mukana monia eri toimijoita, kuten komission omat yksiköt, kansalliset viranomaiset, elinkeinoelämän edustajat ja kuluttajat.

Näiden kysymysten käsittelyssä kiinnitetään huomiota pienten ja keskisuurten yritysten (pk-yritysten) erityistilanteeseen ja siihen, millaisia mahdollisuuksia tai kannustimia niillä on käyttää yksityisyyden suojaa parantavia tekniikoita. Komission olisi käsiteltävä myös sellaisia aiheita kuin luottamus ja tietoisuus, jotka ovat pk-yritysten kannalta erityisen tärkeitä kysymyksiä.

4.1. Ensimmäinen tavoite: Tuki yksityisyyden suojaa parantavien tekniikoiden kehittämiseksi

Jos yksityisyyden suojaa parantavien tekniikoiden käyttöä halutaan laajentaa, niiden suunnittelua, kehittämistä ja valmistamista on lisättävä. Vaikka näin tapahtuukin jo tietystä määrin yksityisellä ja

⁷ Yhdistetyt asiat C-465/00, C-138/01 ja C-139/01, Österreichischer Rundfunk ym. ("Rechnungshof"), yhteisöjen tuomioistuimen tuomio 20.5.2003, Kok. 2003, s. I-04989, 71 ja 72 kohta.

julkisella sektorilla, komissio katsoo, että näitä toimintoja olisi lisättävä. Tämän tavoitteen saavuttaminen edellyttää yksityisyyden suojaa parantaviin tekniikoihin liittyvien tarpeiden ja teknisten vaatimusten kartoittamista ja välineiden kehittämistä osana T&K-toimintaa.

4.1.1. Toimi 1.1: Yksityisyyden suojaa parantaviin tekniikoihin liittyvien tarpeiden ja teknisten vaatimusten kartoittaminen

Yksityisyyden suojaa parantavat tekniikat ovat erittäin riippuvaisia tieto- ja viestintätekniikan alalla tapahtuvasta kehityksestä. Kun tekniikan kehittymiseen liittyvät riskit on kartoitettu, on yksilöitävä tarkoituksenmukaiset vaatimukset teknistä ratkaisua varten.

Komissio kannustaa eri sidosryhmiä kokoontumaan yhteen keskustelemaan yksityisyyden suojaa parantavista tekniikoista. Näitä sidosryhmiä ovat erityisesti tieto- ja viestintätekniikan alan edustajat, yksityisyyden suojaa parantavien tekniikoiden kehittäjät, tietosuojaviranomaiset, lainvalvontaviranomaiset, tekniikan alan yhteistyökumppanit, kuten sähköisten terveydenhuoltopalveluiden ja tietoturva-alan asiantuntijat, kuluttajat ja kansalaisoikeusjärjestöt. Sidosryhmien olisi käytävä säännöllisin väliajoin keskusteluita tekniikan kehittymistä ja uhkia, joita se kohdistaa perusoikeuksiin ja tietosuojaan, sekä kartoitettava näihin uhkiin vastaamiseen liittyviä teknisiä vaatimuksia. Tämä voisi kattaa myös teknisten toimenpiteiden mukauttamisen kulloinkin kyseessä oleviin riskeihin ja tietoihin, ja siinä olisi lisäksi otettava huomioon yleiseen etuun liittyvät näkökohdat, kuten yleinen turvallisuus.

4.1.2. Toimi 1.2: Yksityisyyden suojaa parantavien tekniikoiden kehittäminen

Kun yksityisyyden suojaa parantaviin tekniikoihin liittyvät tarpeet ja tekniset vaatimukset on kartoitettu, on ryhdyttävä konkreettisiin toimiin käyttövalmiin lopputuotteen kehittämiseksi.

Komissio on jo ottanut jossain määrin huomioon yksityisyyden suojaa parantaviin tekniikoihin liittyvät tarpeet. Se tukee tutkimuksen kuudennessa puiteohjelmassa PRIME-hanketta⁸, jossa käsiteltäviä aiheita ovat sähköinen henkilöllisyyden hallinta ja yksityisyyden suojaaminen tietoyhteiskunnassa. OPEN-TC-hankkeessa⁹ kehitetään yksityisyyden suojaa avoimen lähdekoodin ohjelmistotekniikan pohjalta. DISCREET-hankkeen¹⁰ puitteissa kehitetään välitysohjelmistoja yksityisyyden suojaamiseksi kehittyneissä verkkopalveluissa. Jatkossa komissio aikoo tukea seitsemännessä puiteohjelmassa muita T&K-hankkeita ja laaja-alaisia demonstraatioita, joiden tarkoituksena on edistää yksityisyyden suojaa parantavien tekniikoiden käyttöönottoa. Tavoitteena on tarjota perusta käyttäjälähtöisille yksityisyyttä suojaaville palveluille supistamalla Euroopan maiden välisiä oikeudellisia ja teknisiä eroja julkisen ja yksityisen sektorin yhteistyökumppanuuksien avulla.

Komissio kehottaa myös kansallisia viranomaisia ja yksityistä sektoria panostamaan yksityisyyden suojaa parantavien tekniikoiden kehittämiseen. Tämä on ratkaisevan tärkeää, jotta Euroopan teollisuus voisi toimia edelläkävijänä alalla, jonka merkitys kasvaa koko ajan, kun teknisissä standardeissa edellytetään yhä useammin näitä tekniikoita ja myös kuluttajat vaativat niiden käyttöä oikeuksiensa suojaamiseksi verkkoavaruudessa.

⁸ <https://www.prime-project.eu/>.

⁹ <http://www.opentc.net/>.

¹⁰ <http://www.ist-discreet.org/>.

4.2. Toinen tavoite: Yksityiden suojaa parantavien tekniikoiden käytön lisääminen rekisterinpitäjien keskuudessa

Yksityisyyden suojaa parantavista tekniikoista saatavien etujen optimaalinen hyödyntäminen edellyttää sitä, että ne sisällytetään tehokkaasti henkilötietojen käsittelyssä käytettäviin teknisiin laitteisiin ja ohjelmistoihin. Kyseisien laitteiden valmistajien ja niitä tietojenkäsittelyssä käyttävien rekisterinpitäjien osallistumisella onkin tässä suhteessa erityisen suuri painoarvo.

4.2.1. *Toimi 2.1: Yksityisyyden suojaa parantavien tekniikoiden käytön lisääminen elinkeinoelämän alalla*

Komission näkemyksen mukaan kaikki henkilötietojen käsittelyyn osallistuvat tahot hyötyisivät yksityisyyden suojaa parantavien tekniikoiden laajemmasta käytöstä. Tieto- ja viestintätekniikkateollisuus on johtavassa asemassa yksityisyyden suojaa parantavien tekniikoiden kehittäjänä ja toimittajana. Se onkin erityisen tärkeässä asemassa niiden käytön lisäämisessä. Komissio kehottaa kaikkia rekisterinpitäjiä lisäämään ja tehostamaan yksityisyyden suojaa parantavien tekniikoiden käyttöä toimintaprosesseissaan. Tätä varten komissio aikoo järjestää tietoviestintätekniikkateollisuuden keskeisille toimijoille ja erityisesti yksityisyyden suojaa parantavien tekniikoiden kehittäjille suunnattuja seminaareja, joissa pohditaan tapoja, joilla ne voisivat omalta osaltaan edistää yksityisyyden suojaa parantavien tekniikoiden käyttöä rekisterinpitäjien keskuudessa.

Komissio aikoo myös toteuttaa tutkimuksen, jossa tarkastellaan näiden tekniikoiden käytöstä saatavaa taloudellista hyötyä, ja jakaa tutkimustuloksia yrityksille ja erityisesti pk-yrityksille kannustaakseen niitä lisäämään kyseisten tekniikoiden käyttöä.

4.2.2. *Toimi 2.2: Asianmukaisten standardien noudattaminen henkilötietojen suojaamisessa yksityisyyden suojaa parantavien tekniikoiden avulla*

Kattava kampanja yksityisyyden suojaa parantavien tekniikoiden käytön lisäämiseksi edellyttää yksityisyyden suojaa parantavien tekniikoiden valmistamisesta vastaavan tieto- ja viestintätekniikkateollisuuden aktiivista panosta. Asianmukaisten standardien noudattaminen edellyttää kuitenkin eri osapuolten itsesääntelyä tai hyvää tahtoa pidemmälle meneviä toimia. Komissio aikoo selvittää tarkoituksenmukaisten vaikutustenarviointien perusteella, onko tarpeen laatia standardeja henkilötietojen luvalliselle käsittelylle yksityisyyden suojaa parantavilla tekniikoilla. Kyseisten arviointien tulosten perusteella voitaisiin harkita kahdentyypisten välineiden käyttöönottoa:

- *Toimi 2.2.a) Standardointi*

Komissio selvittää, olisiko standardointitoiminnassa otettava huomioon tarve noudattaa tietosuojasääntöjä. Komissio aikoo myös pitää huolen siitä, että sidosryhmien monenvälisen vuoropuhelun tulokset otetaan huomioon sen toimien ja eurooppalaisten standardointielinten työn valmistelussa. Tämä on erityisen tärkeää silloin, kun vuoropuhelussa yksilöidään tarkoituksenmukaisia tietosuojastandardeja, joissa edellytetään tiettyjen yksityisyyden suojaa parantavien tekniikoiden käyttöä.

Komissio saattaa myös pyytää eurooppalaisia standardointielimiä (CEN, CENELEC ja ETSI) arvioimaan Euroopan tasolla ilmeneviä erityistarpeita ja saattamaa ne sen jälkeen kansainväliseen tietoisuuteen eurooppalaisten ja kansainvälisten standardointiorganisaatioiden välillä voimassa olevien sopimusten puitteissa. Eurooppalaisten standardointielinten olisi tarvittaessa laadittava

erillinen standardointia koskeva työohjelma, joka perustuu Euroopan erityistarpeisiin ja täydentää siten kansainvälisellä tasolla meneillään olevaa toimintaa.

- *Toimi 2.2.b) Tietojenkäsittelyyn sovellettavia turvatoimenpiteitä koskevien kansallisten teknisten sääntöjen yhteensovittaminen*

Tietosuojadirektiivin¹¹ nojalla annetussa kansallisessa lainsäädännössä jätetään kansallisille tietosuojaviranomaisille jonkin verran määräysvaltaa teknisten vaatimusten yksityiskohtaisessa määrittämisessä, kuten rekisterinpitäjien ohjeistamisessa, käytössä olevien järjestelmien tarkastelussa tai teknisten ohjeiden antamisessa. Kansalliset tietosuojaviranomaiset voisivat myös edellyttää tiettyjen yksityisyyden suojaa parantavien tekniikoiden lisäämistä tai käyttöä silloin, kun kyseinen henkilötietojen käsittely sitä vaatii. Komission näkemyksen mukaan tällä alalla noudatettavien kansallisten käytäntöjen yhteensovittaminen voisi omalta osaltaan myötävaikuttaa yksityisyyden suojaa parantavien tekniikoiden käytön lisäämiseen. Erityisesti 29 artiklan mukainen työryhmä¹² voisi edistää kyseisten tekniikoiden käyttöä, sillä sen tehtävänä on nimenomaan edistää tietosuojadirektiivin nojalla toteutettujen kansallisten toimenpiteiden yhdenmukaistamista. Komissio kehottaa tämän vuoksi 29 artiklan mukaista työryhmää jatkamaan tätä toimintaa sisällyttämällä työohjelmaansa pysyvästi arviointien laatimisen siitä, olisiko tietojenkäsittelyssä käytettävä yksityisyyden suojaa parantavia tekniikoita, jotka voivat tarjota tehokkaan keinon varmistaa tietosuojasääntöjen noudattaminen. Työryhmän olisi sen jälkeen laadittava kansallisille tietosuojaviranomaisille ohjeet tarkoituksenmukaisten välineiden yhteensovitettua käyttöönottoa varten.

4.2.3. *Toimi 2.3: Yksityisyyden suojaa parantavien tekniikoiden käytön lisääminen viranomaisten keskuudessa*

Viranomaiset sekä jäsenvaltioiden että yhteisön tasolla käsittelevät erittäin usein henkilötietoja hoitaessaan tehtäviään. Viranomaisilla itsellään on velvollisuus kunnioittaa perusoikeuksia ja siten myös oikeutta henkilötietojen suojaan sekä varmistaa, että myös muut kunnioittavat niitä. Niiden olisikin näytettävä hyvää esimerkkiä.

Kansallisten viranomaisten osalta komissio panee merkille, että sähköistä hallintoa varten kehitettyjen sovellusten yleistyminen mahdollistaa julkisten palveluiden tehostamisen. Kuten komission tiedonannossa ”Sähköisen hallinnon merkitys huomisen Euroopassa”¹³ todetaan, yksityisyyden suojaa parantavien tekniikoiden käyttö on välttämätön edellytys sähköisen hallinnon palveluiden menestyksen edellyttämän luottamuksen saavuttamiseksi. Komissio kehottaa hallituksia varmistamaan, että niiden sähköisen hallinnon sovellukset sisältävät tarvittavat tietosuojakeinot. Tämä kattaa myös yksityisyyden suojaa parantavien tekniikoiden mahdollisimman laajan käytön kyseisten sovellusten suunnittelussa ja toteutuksessa.

Yhteisön toimielinten ja elinten osalta komissio varmistaa omasta puolestaan asetuksen (EY) N:o 45/2001 vaatimusten noudattamisen erityisesti lisäämällä yksityisyyden suojaa parantavien tekniikoiden käyttöä tieto- ja viestintätekniikan sovelluksissa, joihin liittyy henkilötietojen käsittelyä. Komissio kehottaa samalla EU:n muita toimielimiä toimimaan samoin. Euroopan tietosuojavaltuutettu voisi antaa yhteisön toimielimille ja elimille neuvoja henkilötietojen käsittelyyn liittyvien sisäisten sääntöjen laatimisesta. Valitessaan uusia tieto- ja

¹¹ Esim. 17 artikla.

¹² Direktiivin 95/46/EY 29 artiklalla perustettu tietosuojatyöryhmä.

¹³ KOM(2003) 567 lopullinen, 26.9.2003.

viestintätekniikkasovelluksia omaan käyttöönsä tai kehittäessään nykyisiä sovelluksia komissio selvittää, voitaisiinko niihin sisällyttää yksityisyyden suojaa parantavia tekniikoita. Yksityisyyden suojaa parantavien tekniikoiden merkitys otetaan huomioon myös komission tietohallintoa koskevassa kokonaisstrategiassa. Komissio pyrkii lisäämään henkilöstönsä tietämystä näistä tekniikoista. Niiden sisällyttäminen komission tieto- ja viestintätekniikkasovelluksiin riippuu kuitenkin kyseisten tuotteiden saatavuudesta ja edellyttää tapauskohtaista, kunkin sovelluksen kehityskaareen perustuvaa arviointia.

4.3. Kolmas tavoite: Kuluttajien kannustaminen käyttämään yksityisyyttä parantavia tekniikoita

Kuluttajat ovat edelleen se ryhmä, jonka kannattaa pitää erityisen tarkkaavaisesti huolta siitä, että henkilötietoja käytetään asianmukaisesti, tietosuojasääntöjä sovelletaan oikein ja yksityisyyden suojaa parantavat tekniikat ovat mahdollisimman tehokkaita.

Kuluttajat olisivatkin saatava tietoisiksi kaikista niistä eduista, joita yksityisyyden suojaa parantavien tekniikoiden käytöstä mahdollisesti saadaan, kun henkilötietojen käsittelyyn liittyviä riskejä saadaan eliminoidua. Heillä olisi lisäksi oltava valmiudet tehdä tietoon perustuvia valintoja ostaessaan tietotekniikkalaitteita ja -ohjelmistoja tai käyttäessään sähköisiä palveluita. Tietoisuus näihin liittyvistä riskeistä on lähtökohtana erityisesti arvioitaessa, tarjoavatko yksityisyyden suojaa parantavat tekniikat riittävän suojan. Käyttäjille onkin annettava selkeää ja ymmärrettävää muodossa olevaa tietoa saatavilla olevista teknisistä välineistä yksityisyyden suojaamiseksi. Yksityisyyden suojaa parantavien tekniikoiden sekä kyseistä tekniikkaa käyttävien sähköisten palveluiden käytön yleistymisen tuottaa taloudellista hyötyä niitä käyttäville aloille. Tämä vaikutus voi heijastua muihin yrityksiin, jotka pyrkivät sen myötä ehkä kiinnittämään enemmän huomiota tietosuojasääntöjen noudattamiseen. Näiden vaikutusten aikaansaaminen edellyttää kuitenkin tiettyjen toimien toteuttamista.

4.3.1. Toimi 3.1: Kuluttajien tietoisuuden lisääminen

Olisi otettava käyttöön johdonmukainen strategia kuluttajien tietoisuuden lisäämiseksi riskeistä, joita henkilötietojen käsittelystä voi aiheutua, ja yksityisyyden suojaa parantavien tekniikoiden näihin ongelmiin mahdollisesti tarjoamista ratkaisuksista. Nämä ratkaisut täydentävät nykyisiä tietosuojalainsäädäntöön sisältyvien korjaustoimenpiteiden järjestelmiä. Komissio aikoo järjestää kattavaa EU:n laajuista tiedotustoimintaa, joiden aiheena on yksityisyyden suojaa parantavien tekniikoiden käyttö.

Päävastuu tästä toiminnasta kuuluu kansallisille tietosuojaviranomaisille, joilla on jo siitä hyödyllistä kokemusta. Komissio kehottaa kansallisia tietosuojaviranomaisia ulottamaan tiedotustoimintansa yksityisyyden suojaa parantavia tekniikoita koskevaan tiedotukseen, jossa olisi käytettävä kaikkia saatavilla olevia välineitä. Komissio pyytää myös 29 artiklan mukaista työryhmää laatimaan johdonmukaisen työohjelman koordinoitakseen käytäntöjä, joita eri jäsenvaltiot noudattavat tietoisuuden lisäämiseksi yksityisyyden suojaa parantavista tekniikoista, sekä toimimaan yhteispisteenä tiedonvaihdossa kansallisella tasolla jo nyt käytössä olevista hyvistä toimintamalleista. Erityisesti kuluttajajärjestöt ja muut toimijat, kuten EU-kuluttajaneuvontakeskusten verkosto (ECC-Net), joka antaa EU:n tasolla kansalaisille neuvoja kuluttajien oikeuksista, voisivat toimia yhteistyössä kuluttajille suunnatun tiedotuksen alalla.

4.3.2. Toimi 3.2: Kuluttajien avustaminen tietoon perustuvien valintojen tekemisessä: Yksityisyyden suojaa koskevat tunnukset

Yksityisyyden suojaa parantavien tekniikoiden käyttöönotto ja käyttö voisi yleistyä, jos käyttäjät voisivat tunnistaa helposti niitä käyttävät tuotteet ja niiden perusominaisuudet. Tätä tarkoitusta varten komissio aikoo tutkia mahdollisuutta ottaa käyttöön EU:n laajuinen yksityisyyden suojaa koskevien tunnusten järjestelmä ja arvioida samalla tällaisen järjestelmän taloudellisia ja yhteiskunnallisia vaikutuksia. Yksityisyyden suojaa koskevien tunnusten tarkoituksena on varmistaa, että kuluttajat voivat helposti tunnistaa tuotteet, joita käyttäessään he voivat olla varmoja siitä, että tietojen käsittelyssä noudatetaan tietosuojasääntöjä ja että tämä on varmistettu erityisesti tarkoituksenmukaisilla yksityisyyden suojaa parantavilla tekniikoilla.

Jotta yksityisyyden suojaa koskevat tunnukset vastaisivat tarkoitustaan, komissio pitää tärkeänä seuraavien periaatteiden noudattamista:

- Yksityisyyden suojaa koskeviin tunnuksiin perustuvien järjestelmien lukumäärä on rajattava minimiin. Liian monien tunnusten olemassaolo voisi aiheuttaa hämmennystä kuluttajien keskuudessa ja heikentää heidän luottamustaan kaikkiin tunnuksiin. Sen vuoksi olisi arvioitava, missä määrin olisi tarkoituksenmukaista sisällyttää eurooppalainen yksityisyyden suojaa koskeva tunnus yleisempään turvallisuusmerkintäjärjestelmään¹⁴.
- Yksityisyyden suojaa koskevat tunnukset olisi myönnettävä ainoastaan sillä edellytyksellä, että tuote täyttää tietosuojasääntöjen mukaiset standardit. Standardien olisi oltava mahdollisimman yhdenmukaiset eri puolella EU:ta.
- Viranomaisten ja erityisesti kansallisten tietosuojaviranomaisten olisi oltava keskeisessä asemassa järjestelmässä osallistumalla relevanttien standardien ja menettelyiden määrittelyyn ja tunnusjärjestelmän toimivuuden seurannassa.

Tämän seurauksena komissio aikoo käydä vuoropuhelua kaikkien sidosryhmien kanssa (esim. kansallisten tietosuojaviranomaisten, toimialajärjestöjen, kuluttajajärjestöjen ja standardointielinten kanssa) hyödyntäen muilla aloilla (esim. ympäristö, maatalous sekä tuotteiden ja palveluiden turvallisuusmerkinnät) saatuja kokemuksia.

¹⁴ Komissio kehotti 31. toukokuuta 2006 antamassaan tiedonannossa ”Turvallisen tietoyhteiskunnan strategia – Lisää vuoropuhelua, yhteistyötä ja vaikutusmahdollisuuksia” (KOM2006) 251 lopullinen) yksityistä sektoria ”luomaan kohtuuhintaiset turvallisuusmerkintäjärjestelmät sellaisille tuotteille, prosesseille ja palveluille, jotka koskevat EU:n erityisiä tarpeita (erityisesti yksityisyyteen liittyen)”.



EUROPEISKA GEMENSKAPERNAS KOMMISSION

Bryssel den 2.5.2007
KOM(2007) 228 slutlig

**MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET OCH
RÅDET**

om främjande av dataskydd genom integritetsfrämjande teknik

MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET OCH RÅDET

om främjande av dataskydd genom integritetsfrämjande teknik

(Text av betydelse för EES)

1. INLEDNING

Den intensiva och ständigt pågående utvecklingen av informations- och kommunikationsteknik (nedan kallad ”IKT”) erbjuder oss hela tiden nya tjänster som förbättrar våra liv. Till stor del är råmaterialet för interaktion i cyberrymden personuppgifter om de enskilda personer som rör sig i cyberrymden när de köper varor och tjänster, inleder eller upprätthåller kontakter med andra eller ger uttryck för sina åsikter på webben. Vid sidan av de fördelar som den här utvecklingen för med sig skapas det också nya risker för den enskilde, exempelvis identitetsstöld, upprättande av diskriminerande profiler, ständig övervakning eller bedrägeri.

Rätten till skydd av personuppgifter fastslås i artikel 8 i Europeiska unionens stadga om de grundläggande rättigheterna. Denna grundläggande rätt kommer till uttryck i EU:s rättsliga ram för skyddet av personuppgifter som framför allt består av dataskyddsdirektivet 95/46/EG¹, direktivet om integritet och elektronisk kommunikation 2002/58/EG² och dataskyddsförordningen (EG) nr 45/2001³ rörande gemenskapsinstitutionernas och gemenskapsorganens databehandling. Denna lagstiftning omfattar flera väsentliga bestämmelser om skyldigheter för registeransvariga och rättigheter för registrerade. Den föreskriver också påföljder och lämpliga åtgärder vid överträdelser och fastställer mekanismer för att genomdriva bestämmelserna i syfte att göra dem effektiva.

Detta system kan emellertid visa sig otillräckligt när personuppgifter sprids i hela världen genom IKT-nät och behandlingen av personuppgifter inbegriper flera jurisdiktioner, ofta utanför EU. I dessa situationer kan de nuvarande bestämmelserna i och för sig anses tillämpliga och ett tydligt rättsligt svar härledas ur dem. Det kan dessutom fastställas vilken behörig myndighet som skall se till att bestämmelserna efterlevs. Det kan emellertid finnas avsevärda praktiska hinder på grund av de svårigheter som är förbundna med den teknik som används, vilket bland annat innebär att uppgifter behandlas av olika aktörer på olika platser, och det kan uppstå svårigheter som är förbundna med verkställigheten av nationella

¹ Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter, EGT L 281, 23.11.1995, s. 31.

² Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation), EGT L 201, 31.7.2002, s. 37.

³ Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter, EGT L 8, 12.1.2001, s. 1.

administrativa utlåtanden och rättsliga avgöranden i andra jurisdiktioner, särskilt i länder utanför EU.

Även om det i egentlig bemärkelse är de registeransvariga som bär det rättsliga ansvaret för att bestämmelserna om dataskydd efterlevs, finns det också andra som till viss del är ansvariga för dataskyddet ur samhälls- och etisk synvinkel. Bland dessa återfinns de som utvecklar tekniska specifikationer och de som konstruerar eller implementerar program eller operativsystem.

Enligt artikel 17 i dataskyddsdirektivet är den registeransvarige skyldig att vidta lämpliga tekniska och organisatoriska åtgärder, och åstadkomma en lämplig säkerhetsnivå i förhållande till arten av de personuppgifter som skall skyddas och de risker som är förknippade med behandlingen av dessa. Att stödja efterlevnaden av lagstiftningen, särskilt när det gäller bestämmelserna om dataskydd, genom användningen av teknik förutses redan till viss del i direktivet om integritet och elektronisk kommunikation⁴.

En ytterligare etapp på vägen mot att förverkliga målet med lagstiftningen, dvs. att minimera behandlingen av personuppgifter och där så är möjligt använda oidentifierade eller pseudonymförsedda uppgifter, skulle kunna få stöd av så kallad integritetsfrämjande teknik (*Privacy Enhancing Technologies*) som skulle göra det lättare att se till att överträdelser av bestämmelserna för dataskydd och kränkningar av den enskildes rättigheter inte bara är förbjudna och leder till påföljder utan också blir svårare rent tekniskt.

Syftet med det här meddelandet, som knyter an till Första rapporten om genomförandet av dataskyddsdirektivet⁵, är att reflektera kring fördelarna med integritetsfrämjande teknik, fastställa kommissionens mål på området för att främja denna teknik, och ange konkreta åtgärder för att uppnå detta mål genom stöd till utvecklingen av integritetsfrämjande teknik och registeransvarigas och övriga konsumenters användning av denna.

2. VAD ÄR INTEGRITETSFRÄMJANDE TEKNIK?

Det finns en rad definitioner av integritetsfrämjande teknik som används i den akademiska världen och inom ramen för pilotprojekt på området. Exempelvis innebär integritetsfrämjande teknik enligt Pisa-projektet, som finansieras av gemenskapen, ett sammanhängande system av IKT-åtgärder som skyddar integriteten genom att ta bort eller reducera personuppgifter eller genom att förhindra onödig eller oönskad behandling av personuppgifter utan att funktionaliteten i informationssystemet går förlorad. Användningen av integritetsfrämjande teknik kan bidra till att informations- och kommunikationssystem och informations- och kommunikationstjänster utformas på ett sådant sätt så att insamlingen och användningen av personuppgifter minimeras och efterlevnaden av bestämmelserna om dataskydd underlättas. Kommissionen säger i sin första rapport om genomförandet av dataskyddsdirektivet att "...användningen av lämpliga tekniska åtgärder är ett nödvändigt komplement till rättsliga åtgärder och att de bör vara en integrerad del i varje ansträngning för att uppnå ett tillräckligt skydd av privatlivet...". Användningen av integritetsfrämjande teknik borde leda till att brott mot vissa dataskyddsbestämmelser blir svårare att genomföra och lättare att upptäcka.

⁴ Skäl 46 och artikel 14.3 i direktiv 2002/58/EG.

⁵ KOM(2003) 265(01), 15.5.2003, se http://eurlex.europa.eu/LexUriServ/site/en/com/2003/com2003_0265en01.pdf

Hur pass effektivt olika former av integritetsfrämjande teknik garanterar att integriteten skyddas, bland annat när det gäller efterlevnaden av lagstiftningen på området, varierar och ändras hela tiden i den dynamiska IKT-världen. De olika formerna har också olika typologi. De kan vara fristående verktyg som kräver en aktiv handling från konsumentens sida (som måste köpa och installera dem i sina datorer) eller ingå i informationssystemens arkitektur. Man kan nämna flera exempel på integritetsfrämjande teknik, bl.a. följande:

- Automatisk anonymisering av uppgifter efter en viss tid stödjer principen om att behandlade uppgifter inte bör sparas i en form som möjliggör identifiering av registrerade längre än vad som är nödvändigt för de ändamål som uppgifterna ursprungligen insamlades för.
- Krypteringsverktyg som förhindrar dataintrång när information skickas över Internet är en hjälp för den registeransvarige när det gäller skyldigheten att vidta lämpliga åtgärder för att skydda personuppgifter mot olaglig behandling.
- Med hjälp av program som blockerar kakor (*cookies*) som placeras på en användares dator för att få datorn att utföra vissa instruktioner utan användarens vetskap, förbättras efterlevnaden av principen om att uppgifter måste behandlas korrekt och lagenligt, och att den registrerade måste informeras om den behandling som pågår.
- P3P (*Platform for Privacy Preferences*), som gör det möjligt för Internetanvändare att analysera webbplatsers policy för integritetsskydd och jämföra dem med sina egna val när det gäller vilka uppgifter som får lämnas, bidrar till att den registrerades samtycke till att hans eller hennes uppgifter behandlas är ett väl underbyggt beslut.

3. KOMMISSIONEN STÖDER INTEGRITETSFRÄMJANDE TEKNIK

Kommissionen anser att integritetsfrämjande teknik bör utvecklas och få en bredare användning, särskilt när personuppgifter behandlas genom IKT-nät. Kommissionen anser att en bredare användning av integritetsfrämjande teknik skulle förbättra integritetsskyddet och bidra till att bestämmelserna om dataskydd följs. Användningen av sådan teknik skulle komplettera den befintliga rättsliga ramen och befintliga genomförandemekanismer.

Kommissionen uppmanade framför allt den privata sektorn att ”*uppmuntra till användning av säkerhetshöjande produkter, förfaranden och tjänster som kan motverka och bekämpa id-stöld och andra angrepp på privatlivets skydd*” i sitt meddelande om en strategi för ett säkert informationssamhälle, KOM(2006) 251 av den 31 maj 2006. Enligt kommissionens plan för en alleuropeisk ram för elektronisk id-hantering 2010⁶ är dessutom en av huvudprinciperna för elektronisk id-hantering att systemet måste vara säkert, omfatta nödvändiga skyddsmekanismer för att skydda användarens integritet och att dess användning skall kunna anpassas till lokala intressen och känsliga frågor.

Det faktum att flera aktörer medverkar i databehandling och att flera olika nationella jurisdiktioner berörs kan försvåra efterlevnaden av den rättsliga ramen. Å andra sidan skulle integritetsfrämjande teknik kunna medföra att vissa brott mot bestämmelserna om dataskydd som resulterar i kränkningar av grundläggande rättigheter, däribland integriteten, undviks

⁶ http://ec.europa.eu/information_society/activities/egovernment_research/doc/eidm_roadmap_paper.pdf

eftersom de tekniskt sett skulle bli svårare att genomföra. Kommissionen är medveten om att teknik, även om den har en avgörande roll när det gäller integritetsskyddet, inte i sig räcker för att skydda integriteten. Integritetsfrämjande teknik måste tillämpas i enlighet med ett regelverk med verkställbara bestämmelser om dataskydd som tillhandahåller flera förhandlingsbara nivåer av integritetsskydd för alla enskilda personer. Användningen av integritetsfrämjande teknik innebär inte att operatörer kan befrias från vissa av sina rättsliga förpliktelser (t.ex. att ge enskilda användare rätt att få tillgång till sina uppgifter).

Viktiga allmänna intressen skulle också kunna tillgodoses bättre. Enligt den rättsliga ramen för dataskydd kan de allmänna principerna begränsas och ingripanden ske i den enskildes rättigheter om viktiga allmänna intressen står på spel som till exempel den allmänna säkerheten, brottsbekämpning eller folkhälsan. Villkoren för sådana begränsningar fastställs i artikel 13 i dataskyddsdirektivet och i artikel 15 i direktivet om integritet och elektronisk kommunikation. De liknar i väsentlig grad villkoren i artikel 8 i europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, nämligen att sådana ingrepp skall göras i enlighet med lagstiftningen, stå i proportion till sitt syfte och vara nödvändiga i ett demokratiskt samhälle med hänsyn till viktiga allmänna intressen⁷. Användningen av integritetsfrämjande teknik bör inte hindra brottsbekämpande organ eller andra behöriga myndigheter från att ingripa inom ramen för ett lagligt utövande av deras uppgifter för ett allmänt intresse, t.ex. för att bekämpa IT-brottslighet eller terrorism eller förhindra spridningen av smittsamma sjukdomar. De ansvariga myndigheterna bör kunna få tillgång till personuppgifter när detta är nödvändigt för dessa syften och i enlighet med de förfaranden, villkor och garantier som anges i lagstiftningen.

Bättre efterlevnad av bestämmelserna om dataskydd skulle också ha en positiv inverkan på konsumenternas förtroende, särskilt för cyberrymden. Ett antal lovande mervärdestjänster som är beroende av överföring av personuppgifter över IT-nät, t.ex. e-lärande, e-förvaltning, e-hälsovård, e-banktjänster, e-handel eller system för den s.k. intelligenta bilen, skulle med all säkerhet gynnas. Människor skulle kunna vara säkra på att de uppgifter som de lämnar för att identifiera sig, ta emot tjänster eller göra betalningar bara används för berättigade ändamål och att deras deltagande i det digitala samhället inte sker på bekostnad av deras rättigheter.

4. TIDIGARE OCH KOMMANDE ÅTGÄRDER

I sin strävan att stärka integritetsskyddet och skyddet av personuppgifter i gemenskapen, bland annat genom att främja utvecklingen och användningen av integritetsfrämjande teknik, planerar kommissionen att vidta följande åtgärder med deltagande av en rad olika aktörer, bland annat kommissionens egna avdelningar, nationella myndigheter, näringslivet och konsumenter.

Under diskussionerna kommer de små och medelstora företagens speciella situation att uppmärksammas liksom deras möjligheter och motivation för att använda integritetsfrämjande teknik. Kommissionen bör också ta upp frågor som t.ex. förtroende och medvetenhet, som är av särskild vikt för små och medelstora företag.

⁷ EG-domstolens dom av den 20 maj 2003, förenade målen C-465/00, C-138/01 och C-139/01, ”Österreichischer Rundfunk m.fl”. (”Rechnungshof”), REG 2003, s. I-4989, punkterna 71 och 72.

4.1. Mål 1: stödja utvecklingen av integritetsfrämjande teknik

Om integritetsfrämjande teknik skall kunna användas mer allmänt måste den först och främst utformas, utvecklas och tillverkas. Även om detta redan pågår i viss utsträckning både inom den offentliga och den privata sektorn anser kommissionen att denna verksamhet bör intensifieras. Mot denna bakgrund bör behovet av integritetsfrämjande teknik och de tekniska kraven för denna fastställas, och nya verktyg bör utvecklas genom forskning och teknisk utveckling.

4.1.1. Åtgärd 1.1: Fastställa behoven av integritetsfrämjande teknik och de tekniska kraven för denna

Integritetsfrämjande teknik är i stor utsträckning beroende av utvecklingen av informations- och kommunikationsteknik. När väl riskerna med den tekniska utvecklingen konstaterats måste de lämpliga kraven på en teknisk lösning fastställas.

Kommissionen kommer att uppmuntra olika grupper av aktörer att samlas och diskutera integritetsfrämjande teknik. Dessa grupper kommer framför allt att omfatta representanter från IKT-sektorn, utvecklare av integritetsfrämjande teknik, dataskyddsmyndigheter, brottsbekämpande organ, parter på det tekniska området däribland experter från relevanta områden som t.ex. e-hälsovård eller informationssäkerhet, konsumentorganisationer och organisationer för medborgerliga rättigheter. Dessa aktörer bör regelbundet se närmare på teknikens utveckling, upptäcka de risker den medför för grundläggande rättigheter och dataskydd samt ange de viktigaste tekniska krav som bör ställas på en lösning som bygger på integritetsfrämjande teknik. Dessa kan omfatta att finslipa de tekniska åtgärderna med hänsyn till de olika risker och de olika typer av uppgifter som det gäller och med hänsyn till behovet av att skydda allmänna intressen, t.ex. den allmänna säkerheten.

4.1.2. Åtgärd 1.2: Utveckla integritetsfrämjande teknik

När behovet av denna teknik och dess tekniska krav fastställts måste det till konkreta åtgärder för att åstadkomma en slutprodukt som är klar för användning.

Kommissionen har redan tagit upp behovet av integritetsfrämjande teknik. Inom ramen för det sjätte ramprogrammet sponsrar den Primeprojektet⁸ som behandlar frågor om digital id-hantering och integritet i informationssamhället. Projektet OPEN-TC⁹ möjliggör skydd av personuppgifter baserat på öppen och säker databehandling och projektet Discreet¹⁰ utvecklar mellanprogram för att stärka integritetsskyddet i avancerade nätverkstjänster. Kommissionen avser att i framtiden, inom ramen för det sjunde ramprogrammet, stödja andra projekt inom forskning och teknisk utveckling och omfattande pilotdemonstrationer i syfte att utveckla och öka intresset för integritetsfrämjande teknik. Syftet är att skapa en grund för integritetsfrämjande tjänster som ger användarna större inflytande och som utjämnar de rättsliga och tekniska olikheterna i Europa genom offentlig-privata partnerskap.

Kommissionen uppmanar även nationella myndigheter och den privata sektorn att investera i utvecklingen av integritetsfrämjande teknik. Sådana investeringar är av avgörande betydelse för att placera den europeiska industrin främst inom en sektor som kommer att växa

⁸ <https://www.prime-project.eu/>

⁹ <http://www.opentc.net/>

¹⁰ <http://www.ist-discreet.org/>

allteftersom sådan teknik i allt större utsträckning kommer att krävas i tekniska standarder och efterfrågas av konsumenter som är mer medvetna om behovet av att skydda sina rättigheter i cyberrymden.

4.2. Mål 2: Stödja registeransvarigas användning av integritetsfrämjande teknik

Integritetsfrämjande teknik kommer bara att komma till verklig nytta om den effektivt byggs in i och används i teknisk utrustning och programverktyg som behandlar personuppgifter. Deltagande av den industri som tillverkar sådan utrustning och av registeransvariga som använder sig av denna vid databehandling är därför av avgörande betydelse.

4.2.1. Åtgärd 2.1: *Främja näringslivets användning av integritetsfrämjande teknik*

Kommissionen anser att en ökad användning av integritetsfrämjande teknik skulle gagna alla som sysslar med behandling av personuppgifter. IKT-industrin, i sin egenskap av den främste utvecklaren och leverantören av integritetsfrämjande teknik, spelar en särskilt viktig roll när det gäller att främja sådan teknik. Kommissionen uppmanar alla registeransvariga att mer allmänt och i högre grad integrera och tillämpa integritetsfrämjande teknik i sitt arbete. Kommissionen kommer i detta syfte att anordna seminarier med huvudaktörer inom IKT-industrin, särskilt utvecklare av integritetsfrämjande teknik, för att undersöka hur de skulle kunna bidra till att främja användningen av tekniken bland registeransvariga.

Kommissionen kommer också att göra en undersökning av de ekonomiska vinsterna med integritetsfrämjande teknik och sprida resultaten i syfte att uppmuntra företag, i synnerhet små och medelstora företag, att använda tekniken.

4.2.2. Åtgärd 2.2: *Se till att lämpliga standarder för skydd av personuppgifter tillgodoses genom integritetsfrämjande teknik*

På samma sätt som en omfattande kampanj för att främja användningen av integritetsfrämjande teknik kräver aktivt deltagande från IKT-industrin i dess egenskap av tillverkare, krävs det för att lämpliga standarder skall följas insatser utöver självreglering eller de berörda aktörernas goda vilja. Kommissionen kommer att genom lämpliga konsekvensanalyser bedöma behovet av att ta fram standarder för laglig behandling av personuppgifter med integritetsfrämjande teknik. På grundval av resultaten av konsekvensanalyserna kommer följande två typer av verktyg att övervägas:

- **Åtgärd 2.2.a) Standardisering**

Kommissionen kommer undersöka behovet av att efterlevnad av bestämmelserna för dataskydd beaktas vid standardiseringsarbete. Kommissionen kommer också att sträva efter att ta hänsyn till de åsikter som framförs vid aktörernas diskussioner om integritetsfrämjande teknik när den förbereder sina egna åtgärder på området och till det arbete som utförs vid de europeiska standardiseringsorganen. Detta kommer att vara avgörande, särskilt om det vid diskussionerna fastställs lämpliga standarder för dataskydd som kräver integrering och användning av viss integritetsfrämjande teknik.

Kommissionen kan uppmana de europeiska standardiseringsorganen (CEN, Cenelec, Etsi) att bedöma särskilda europeiska behov och därefter lyfta upp dessa till internationell nivå genom att tillämpa befintliga avtal mellan europeiska och internationella standardiseringsorgan. När så är lämpligt bör de europeiska standardiseringsorganen upprätta ett särskilt arbetsprogram

för standardisering som täcker de europeiska behoven och på så sätt komplettera det pågående arbetet på internationell nivå.

- *Åtgärd 2.2.b Samordning av nationella tekniska bestämmelser när det gäller säkerhetsåtgärder för databehandling*

Nationell lagstiftning som antagits i enlighet med dataskyddsdirektivet¹¹ ger nationella dataskyddsmyndigheter visst inflytande när det gäller att fastställa precisa tekniska krav, t.ex. när det gäller att utarbeta vägledning för registeransvariga, granska de system som inrättas eller utfärda tekniska anvisningar. De nationella dataskyddsmyndigheterna skulle också kunna kräva att viss integritetsfrämjande teknik införlivas och används när behandlingen av personuppgifter kräver detta. Kommissionen anser detta som ett område där samordning av nationell praxis skulle kunna bidra positivt till att främja användningen av integritetsfrämjande teknik. Särskilt artikel 29-gruppen¹², vars roll är att arbeta för en enhetlig tillämpning av nationella bestämmelser som antas inom ramen för direktivet, skulle kunna bidra till detta. Kommissionen uppmanar därför artikel 29-gruppen att fortsätta sitt arbete på området och att i sitt program inkludera ett permanent inslag, nämligen analys av om integritetsfrämjande teknik behöver integreras vid behandling av personuppgifter som ett effektivt sätt att säkerställa att bestämmelserna för dataskydd efterlevs. Detta arbete bör sedan leda till riktlinjer för dataskyddsmyndigheter som skall genomföras på nationell nivå genom ett samordnat antagande av lämpliga instrument.

4.2.3. Åtgärd 2.3: Främja de offentliga myndigheternas användning av integritetsfrämjande teknik

Offentliga myndigheter, både på nationell nivå och på EU-nivå, genomför i utövandet av sina befogenheter flera uppgiftsbehandlingsprocesser som omfattar personuppgifter. Offentliga organ måste själva respektera de grundläggande rättigheterna, bland annat rätten till skydd av personuppgifter, och se till att andra respekterar dem. De bör därför föregå med gott exempel.

När det gäller de nationella myndigheterna konstaterar kommissionen att program för e-förvaltning används i allt större utsträckning som ett sätt att effektivisera de offentliga tjänsterna. Enligt *kommissionens meddelande om e-förvaltningens roll i Europas framtid*¹³, är det nödvändigt att använda integritetsfrämjande teknik inom e-förvaltningen för att skapa den tilltro och det förtroende som krävs för att e-förvaltningen skall bli en framgång. Kommissionen uppmanar regeringarna att sörja för att mekanismer för dataskydd ingår i de program som används inom e-förvaltningen, bland annat genom att integritetsfrämjande teknik används i så stor utsträckning som möjligt både vid utformningen och implementeringen av programmen.

När det gäller gemenskapsinstitutioner och gemenskapsorgan kommer kommissionen att se till att den själv uppfyller kraven i förordning (EG) nr 45/2001, framför allt genom en ökad användning av integritetsfrämjande teknik vid implementeringen av IKT-program som innebär behandling av personuppgifter. Kommissionen uppmanar också övriga EU-institutioner att göra på samma sätt. Europeiska datatillsynsmannen skulle kunna bidra med rådgivning till gemenskapsinstitutionerna och gemenskapsorganen genom att utarbeta interna

¹¹ T.ex. artikel 17.

¹² Den arbetsgrupp för skydd av enskilda med avseende på behandlingen av personuppgifter som inrättas genom artikel 29 i direktiv 95/46/EG.

¹³ KOM(2003) 567 slutlig, 26.9.2003.

regler för behandling av personuppgifter. När kommissionen väljer nya IKT-program för eget bruk eller vidareutvecklar befintliga program kommer den att överväga möjligheten att införa integritetsfrämjande teknik. Betydelsen av integritetsfrämjande teknik kommer att återspeglas i kommissionens övergripande strategi för IT-förvaltning. Kommissionen kommer också att fortsätta att medvetandegöra sin personal. Implementeringen av integritetsfrämjande teknik i kommissionens IKT-program beror emellertid på tillgången på motsvarande produkter och måste bedömas i varje enskilt fall, mot bakgrund av i vilken utvecklingsfas programmet befinner sig.

4.3. Mål III: Uppmuntra konsumenterna att använda integritetsfrämjande teknik

Konsumenterna förblir den grupp som har störst intresse av att deras personuppgifter används korrekt, att dataskyddsbestämmelser antas på ett korrekt sätt och att integritetsfrämjande teknik ger effektiva garantier för detta.

Konsumenter bör därför bli fullt medvetna om de fördelar som användningen av integritetsfrämjande teknik kan innebära för att minska riskerna vid transaktioner som innebär behandling av personuppgifter. När de köper IT-utrustning och program eller använder e-tjänster, bör de också kunna göra ett väl underbyggt val. Deras val bör visa att de är medvetna om riskerna, särskilt om huruvida integritetsfrämjande teknik erbjuder lämpligt skydd. Det måste därför finnas enkel och lättfattlig information för konsumenterna om vilka tekniska verktyg som kan skydda integriteten. En ökad användning av integritetsfrämjande teknik och av e-tjänster med inbyggd integritetsfrämjande teknik betyder i sin tur ekonomisk vinst för de företag som använder dem och kan skapa en snöbollseffekt, som uppmuntrar andra företag att lägga större vikt vid att följa bestämmelserna för dataskydd. För att uppnå detta måste en rad åtgärder vidtas.

4.3.1. Åtgärd 3.1: Medvetandegöra konsumenterna

Det bör antas en samlad strategi som syftar till att medvetandegöra konsumenter om riskerna i samband med behandling av deras personuppgifter och om de lösningar som den integritetsfrämjande tekniken kan erbjuda som ett komplement till de befintliga systemen för korrigerande åtgärder i dataskyddslagstiftningen. Kommissionen planerar att inleda en rad EU-omfattande medvetandehöjande åtgärder när det gäller integritetsfrämjande teknik.

Huvudansvaret för detta ligger på nationella dataskyddsmyndigheter som redan har relevanta erfarenheter på området. De uppmanas av kommissionen att öka sina medvetandehöjande åtgärder för att på alla tänkbara sätt informera om integritetsfrämjande teknik. Kommissionen uppmanar också artikel 29-gruppen att samordna nationell praxis i en sammanhängande arbetsplan för att öka medvetenheten om integritetsfrämjande teknik och att fungera som mötesplats för utbyte av god praxis som redan tillämpas nationellt. Framför allt skulle konsumentorganisationer och andra aktörer, t.ex. nätverket av europeiska konsumentcentrum i sin egenskap av ett EU-omfattande nätverk för att rådgivning till medborgarna om deras rättigheter som konsumenter, kunna vara partner i arbetet med utbilda konsumenterna.

4.3.2. Åtgärd 3.2: Underlätta för konsumenterna att göra ett väl underbyggt val: integritetsmärkning

Spridningen och användningen av integritetsfrämjande teknik skulle främjas om det var lätt att känna igen förekomsten av sådan i en viss produkt och teknikens grundläggande drag. Kommissionen planerar därför att undersöka möjligheterna för ett EU-omfattande system för

integritetsmärkning, vilket också skulle omfatta en konsekvensanalys ur ekonomisk och samhällelig synvinkel. Integritetsmärkning skulle syfta till att konsumenterna lätt kan konstatera om en viss produkt ger garantier för eller bidrar till att dataskyddsbestämmelserna efterlevs vid behandling av personuppgifter, särskilt genom att produkten omfattar lämplig integritetsfrämjande teknik.

Kommissionen anser att följande principer bör följas för att integritetsmärkningen skall uppnå sitt mål:

- Antalet system för integritetsmärkning bör begränsas till ett minimum. Alltför många integritetsmärkningar skulle i själva verket skapa mer förvirring för konsumenterna och undergräva deras förtroende för märkningen. Det bör därför bedömas om och i hur hög grad det vore lämpligt att integrera en europeisk integritetsmärkning i ett mer allmänt system för säkerhetscertifiering¹⁴.
- Integritetsmärkning bör bara beviljas en viss produkt om denna uppfyller en rad standarder som motsvarar dataskyddsbestämmelser. Dessa standarder bör vara så enhetliga som möjligt i hela EU.
- Offentliga myndigheter, särskilt nationella dataskyddsmyndigheter, bör spela en viktig roll i systemet genom att delta vid framtagningen av relevanta standarder och förfaranden och i övervakningen av att märkningssystemet fungerar.

Kommissionen kommer med detta i åtanke och med hänsyn till tidigare erfarenheter när det gäller märkning på andra områden (t.ex. miljö, jordbruk, säkerhetscertifiering för produkter och tjänster) att hålla dialog med samtliga berörda parter, däribland nationella dataskyddsmyndigheter, näringslivets organisationer och konsumentorganisationer samt standardiseringsorgan.

¹⁴ Redan i sitt meddelande av den 31 maj 2006 om en strategi för ett säkert informationssamhälle – ”Dialog, partnerskap och användarinflytande” (KOM(2006) 251 slutlig) uppmanade kommissionen den privata sektorn att ”sträva efter betalbara system för säkerhetscertifiering för produkter, processer och tjänster som kan uppfylla EU:s särskilda behov (inte minst i fråga om skydd av privatlivet)”.