IETEIKUMI

KOMISIJA

KOMISIJAS IETEIKUMS

(2009. gada 12. maijs)

par privātuma un datu aizsardzības principu īstenošanu saistībā ar radiofrekvenciālās identificēšanas lietojumiem

(izziņots ar dokumenta numuru C(2009) 3200)

(2009/387/EK)

EIROPAS KOPIENU KOMISIJA,

ņemot vērā Eiropas Kopienas dibināšanas līgumu un jo īpaši tā 211. pantu,

apspriedusies ar Eiropas Datu aizsardzības uzraudzītāju,

tā kā:

(1) Radiofrekvenciālā identifikācija (*RFID*) ir jauns informācijas sabiedrības attīstības virziens, kura ietvaros par neatņemamu ikdienas sastāvdaļu aizvien plašāk kļūs priekšmeti, kas aprīkoti ar mikroelektronikas ierīcēm, kuras spēj automātiski apstrādāt datus.

(2) *RFID* tiek izmantota aizvien plašāk un tādējādi kļūst par ikdienas dzīves sastāvdaļu virknē jomu, piemēram, loģistikā [1], veselības aprūpē, sabiedriskajā transportā, mazumtirdzniecībā (jo īpaši saistībā ar produktu drošuma uzlabošanu un produktu ātrāku izņemšanu no tirgus), izklaidē, darbā, ceļu nodevu iekasēšanas pārvaldībā, bagāžas pārvaldībā un ceļojuma dokumentos.

(3) Pateicoties tam, ka *RFID* tehnoloģija ir ļoti perspektīva ekonomikas jomā, kur tā var radīt jaunas uzņēmējdarbības iespējas, samazināt izmaksas un uzlabot efektivitāti, jo īpaši saistībā ar viltošanas apkarošanu un e-atkritumu, bīstamu materiālu un pārstrādātu produktu pārvaldīšanu to aprites cikla beigās, tai ir iespēja kļūt par jaunu izaugsmes un darba vietu radīšanas virzītājspēku, tādējādi ievērojami sekmējot Lisabonas stratēģijas mērķu sasniegšanu.

(4) *RFID* tehnoloģija ļauj no neliela attāluma, bez redzamas mijiedarbības ar *RFID* marķējumu un bez fiziskas saskares starp lasītāju vai rakstītāju un šādu marķējumu īstenot datu, tostarp personas datu, apstrādi. Tādējādi attiecīgā persona var nezināt, ka šāda mijiedarbība notiek.

(5) *RFID* iespējams izmantot arī, lai apstrādātu datus, kas attiecas uz identificētu vai identificējamu fizisku personu, to identificējot tieši vai netieši. Šādam lietojumam paredzētas sistēmas var apstrādāt marķējumā saglabātus personas datus, piemēram, personas vārdu, dzimšanas datumu vai adresi, biometriskos datus vai datus, kas sasaista *RFID* priekšmeta numuru ar sistēmā citviet saglabātiem personas datiem. Turklāt šo tehnoloģiju potenciāli var izmantot tādu personu uzraudzīšanai, kuru īpašumā atrodas viens vai vairāki priekšmeti ar *RFID* priekšmeta numuru.

(6) *RFID* marķējumu iespējams nemanāmā veidā izvietot it visur, tāpēc, izmantojot šo tehnoloģiju, īpaša uzmanība jāpievērš ar privātumu un datu aizsardzību saistītiem jautājumiem. Tāpēc, pirms tiek plaši uzsākta *RFID* izmantošana, sistēmā jāiestrādā privātuma un informācijas drošības funkcijas ("konstrukcijā iekļautas drošības un privātuma" princips).

(7) Daudzos ieguvumus ekonomikas un sociālajā jomā *RFID* spēs nodrošināt tikai tad, ja būs īstenoti efektīvi pasākumi personas datu un privātuma aizsardzībai, kā arī atrisināti ar to saistītie ētiskie principi, kas ir galvenais temats diskusijās par to, vai *RFID* tehnoloģija ir pieņemama sabiedrībai.

(8) Dalībvalstīm un ieinteresētajām personām jo īpaši šajā *RFID* ieviešanas sākumposmā vajadzētu veikt papildu darbības, lai nodrošinātu, ka *RFID* lietojumus uzrauga un ka tiek ievērotas personu tiesības un brīvības.

[1] COM(2007) 607, galīgā redakcija.

(9) Komisijas 2007. gada 15. marta paziņojumā "Radiofrekvenču identifikācija (*RFID*) Eiropā: ceļā uz politikas īstenošanas pasākumiem" [1] teikts, ka Komisija ar vienu vai vairākiem ieteikumiem precizēs un sniegs vadlīnijas par datu aizsardzības un privātuma aspektiem *RFID* lietojumos.

(10) *RFID* lietojumiem, kas apstrādā personas datus, pilnībā piemēro tiesības un pienākumus saistībā ar personas datu aizsardzību un šādu datu brīvu apriti, kā paredzēts Eiropas Parlamenta un Padomes 1995. gada 24. oktobra Direktīvā 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti [2] un Eiropas Parlamenta un Padomes 2002. gada 12. jūlija Direktīvā 2002/58/EK par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektronisko komunikāciju) [3].

(11) Eiropas Parlamenta un Padomes 1999. gada 9. marta Direktīvā 1999/5/EK par radioiekārtām un telekomunikāciju termināla iekārtām un to atbilstības savstarpējo atzīšanu [4] noteiktie principi būtu jāpiemēro, izstrādājot *RFID* lietojumus.

(12) Eiropas Datu aizsardzības uzraudzītāja atzinumā [5] ietverti norādījumi, kā rīkoties ar izstrādājumiem, kuriem pievienots marķējums un kuri nonāk personu īpašumā, un aicināts veikt privātuma un drošības ietekmes novērtējumus, lai noteiktu un izstrādātu "labākos pieejamos paņēmienus", kā nodrošināt *RFID* sistēmu privātumu un drošību.

(13) *RFID* lietojuma operatoriem būtu jāveic visi nepieciešamie pasākumi, lai nodrošinātu, ka datus ne ar kādiem līdzekļiem, kurus varētu izmantot vai nu *RFID* lietojuma operators, vai jebkura cita persona, nebūtu iespējams piesaistīt identificētai vai identificējamai fiziskai personai, izņemot, ja šādus datus apstrādā atbilstīgi piemērojamajiem principiem un tiesību normām attiecībā uz datu aizsardzību.

(14) Komisijas 2007. gada 2. maija paziņojumā "Datu aizsardzības veicināšana, izmantojot privātuma uzlabojošas tehnoloģijas (PUT)" [6] ir skaidri noteikts, ka, lai samazinātu personas datu apstrādi un vienmēr, kad iespējams, izmantotu anonīmus vai pseidoanonīmus datus, jāatbalsta PUT izstrādāšana un tas, ka PUT izmanto par datu apstrādi atbildīgās personas un fiziskas personas.

(15) Komisijas 2006. gada 31. maija paziņojumā "Drošas informācijas sabiedrības stratēģija – Dialogs, partnerība un iespējas" [7] atzīts, ka dažādība, atvērtība, savietojamība, izmantojamība un konkurence ir svarīgs informācijas sabiedrības virzītājspēks, uzsvērta dalībvalstu un valsts pārvaldes loma, lai uzlabotu izpratni un veicinātu labu drošības paņēmienu izmantošanu, kā arī izteikts aicinājums privātā sektora ieinteresētajām personām sākt rīkoties, lai izveidotu izmaksu ziņā pieejamas drošības sertifikācijas shēmas produktiem, procesiem un pakalpojumiem saistībā ar konkrētiem lietojumiem ES, jo īpaši attiecībā uz privātumu.

(16) Padomes 2007. gada 22. marta Rezolūcijā par drošas informācijas sabiedrības stratēģiju Eiropā [8] dalībvalstis tiek aicinātas veltīt pienācīgu uzmanību nepieciešamībai nepieļaut jaunus un cīnīties ar esošajiem drošības apdraudējumiem elektronisko sakaru tīklos.

(17) Kopienas līmenī izstrādāta sistēma privātuma un datu aizsardzības ietekmes novērtējumu īstenošanai nodrošinās, ka visas dalībvalstis saskaņoti ievēros šo ieteikumu. Šādas sistēmas izveidošanai vajadzētu pamatoties uz pašreizējo praksi un pieredzi, kas gūta dalībvalstīs un trešās valstīs, kā arī darbu, ko veikusi Eiropas Tīklu un informācijas drošības aģentūra (*ENISA*) [9].

(18) Komisija nodrošinās vadlīniju izstrādāšanu Kopienas līmenī par informācijas drošības pārvaldību *RFID* lietojumos, pamatojoties uz pašreizējo praksi un pieredzi, kas gūta dalībvalstīs un trešās valstīs. Dalībvalstīm vajadzētu piedalīties šajā procesā un iedrošināt piedalīties privātas struktūras un iestādes.

(19) Pirms ieviest *RFID* lietojumu, operatora īstenots privātuma un datu aizsardzības ietekmes novērtējums nodrošinās informāciju, kas nepieciešama, lai veiktu atbilstošus aizsardzības pasākumus. Šādi pasākumi būs jāuzrauga un jāpārskata visā *RFID* lietojuma ekspluatācijas laikā.

(20) Mazumtirdzniecības nozarē privātuma un datu aizsardzības ietekmes novērtējumam attiecībā uz izstrādājumiem ar *RFID* marķējumu, kurus pārdod patērētājiem, vajadzētu nodrošināt nepieciešamo informāciju, lai noteiktu, vai ir iespējams privātuma vai personas datu aizsardzības apdraudējums.

---

[1] COM(2007) 96, galīgā redakcija.
[2] OV L 281, 23.11.1995., 31. lpp.
[3] OV L 201, 31.7.2002., 37. lpp.
[4] OV L 91, 7.4.1999., 10. lpp.
[5] OV C 101, 23.4.2008., 1. lpp.
[6] COM(2007) 228, galīgā redakcija.
[7] COM(2006) 251, galīgā redakcija.
[8] OV C 68, 24.3.2007., 1. lpp.
[9] Eiropas Parlamenta un Padomes Regulas (EK) Nr. 460/2004 2. panta 1. punkts (OV L 77, 13.3.2004., 1. lpp.).

(21) Informācijas drošības un privātuma pasākumus visā ar *RFID* izmantošanu saistītajā uzņēmējdarbības procesā var palīdzēt pārvaldīt starptautisku standartu (piemēram tādu, ko izstrādājusi Starptautiskā Standartizācijas organizācija (*ISO*)), rīcības kodeksu un ES normatīvajai bāzei atbilstošas labākās prakses izmantošana.

(22) *RFID* lietojumiem, kas skar sabiedrību kopumā, piemēram, elektroniskās biļetes sabiedriskajā transportā, ir nepieciešami piemēroti aizsargpasākumi. Attiecībā uz informācijas drošību un privātumu īpaši būtiski ir tādi *RFID* lietojumi, kas ietekmē privātpersonas, piemēram, ja tiek apstrādāti to biometriskie identifikācijas dati vai ar veselību saistīti dati, un tāpēc tiem jāpievērš pastiprināta uzmanība.

(23) Sabiedrībai kopumā jāapzinās pienākumi un tiesības, kas piemērojamas saistībā ar *RFID* lietojumiem. Tāpēc to pušu pienākums, kuras ievieš šo tehnoloģiju, ir informēt attiecīgās personas par šādiem lietojumiem.

(24) Sabiedrības un mazo un vidējo uzņēmumu (MVU) informēšana par *RFID* funkcijām un iespējām palīdzēs pilnvērtīgi izmantot šīs tehnoloģijas ekonomisko potenciālu, vienlaicīgi mazinot risku, ka to varētu izmantot sabiedrībai nevēlamā veidā, un padarot to pieņemamāku iedzīvotājiem.

(25) Komisija piedalīsies šā ieteikuma īstenošanā tieši un netieši, veicinot dialogu un sadarbību starp ieinteresētajām personām, jo īpaši – izmantojot Konkurētspējas un jauninājumu pamatprogrammu (KJP), kas izveidota ar Eiropas Parlamenta un Padomes Lēmumu Nr. 1639/2006/EK ([1]), un Septīto pētniecības pamatprogrammu (*FP7*), kas izveidota ar Eiropas Parlamenta un Padomes Lēmumu Nr. 1982/2006/EK ([2]).

(26) Kopienas līmenī ir būtiski pētīt un attīstīt privātumu uzlabojošas zemu izmaksu tehnoloģijas un informācijas drošības tehnoloģijas, lai veicināto to plašāku ieviešanu ar pieņemamiem nosacījumiem.

(27) Šajā ieteikumā ir ievērotas pamattiesības un principi, kas jo īpaši atzīti Eiropas Savienības Pamattiesību hartā. Šā ieteikuma mērķis jo īpaši ir nodrošināt to, ka pilnībā tiek ņemts vērā privātums un ģimenes dzīve, un personas datu aizsardzība,

([1]) OV L 310, 9.11.2006., 15. lpp.
([2]) OV L 412, 30.12.2006., 1. lpp.

AR ŠO IESAKA.

Ieteikuma joma

1. Šajā ieteikumā sniegti norādījumi dalībvalstīm par to, kā projektēt un ekspluatēt *RFID* lietojumus likumīgā, ētiski, sociāli un politiski pieņemamā veidā, ievērojot tiesības uz privātumu un nodrošinot personas datu aizsardzību.

2. Šajā ieteikumā sniegti norādījumi par pasākumiem, kas veicami *RFID* lietojumu ieviešanai, lai nodrošinātu, ka, tos ieviešot, tiktu ievēroti tie valstu tiesību akti, ar kuriem ievieš Direktīvu 95/46/EK, Direktīvu 1999/5/EK un Direktīvu 2002/58/EK (ja tādi ir).

Definīcijas

3. Šajā ieteikumā piemēro Direktīvā 95/46/EK noteiktās definīcijas. Piemēro arī šādas definīcijas:

a) "radiofrekvenciālā identifikācija" (*RFID*) ir elektromagnētiskā starojuma viļņu vai reaktīvās induktīvās saites (*reactive field coupling*) izmantošana spektra radiofrekvenču daļā, lai nodrošinātu sakarus ar marķējumu, izmantojot dažādas modulācijas un kodēšanas shēmas, lai unikālā veidā nolasītu radiofrekvenciālā marķējuma identitāti vai citus tajā saglabātos datus;

b) "*RFID* marķējums" jeb "marķējums" ir vai nu *RFID* ierīce, kura spēj ģenerēt radiosignālu, vai arī *RFID* ierīce, kura (atkarībā no ierīces veida) atpakaļsavieno, atpakaļizplata vai atstaro un modulē nesējsignālu, kas saņemts no lasītāja vai rakstītāja;

c) "*RFID* lasītājs vai rakstītājs" jeb "lasītājs" ir stacionāra vai mobila datu uztveršanas un identifikācijas ierīce, kas izmanto radiofrekvences spektra elektromagnētiskos viļņus vai reaktīvo induktīvo saiti (*reactive field coupling*), lai ierosinātu un nodrošinātu modulētu datu saņemšanu no marķējuma vai marķējumu grupas;

d) "*RFID* lietojums" jeb "lietojums" ir lietojums, kad, izmantojot marķējumu un lasītājus, tiek apstrādāti dati un kuru atbalsta ar papildsistēmu un sakaru tīkla infrastruktūru;

e) "*RFID* lietojuma operators" jeb "operators" ir fiziska vai juridiska persona, iestāde, aģentūra vai jebkura cita struktūra, kas atsevišķi vai kopā ar citām nosaka, kāds ir lietojuma mērķis un izmantojamie līdzekļi, tostarp par personas datu apstrādi atbildīgās personas *RFID* lietojumā;

f) "informācijas drošība" ir informācijas konfidencialitātes, integritātes un pieejamības saglabāšana;

g) "uzraudzība" ir jebkura darbība, ko īsteno ar mērķi noteikt, novērot, kopēt vai reģistrēt datus par personas atrašanās vietu, pārvietošanos, darbības vai stāvokli.

Privātuma un datu aizsardzības ietekmes novērtējumi

4. Dalībvalstīm būtu jānodrošina, ka nozare sadarbībā ar attiecīgām pilsoniskās sabiedrības ieinteresētajām personām sagatavo privātuma un datu aizsardzības ietekmes novērtējuma sistēmu. Šī sistēma iesniedzama apstiprināšanai 29. panta datu aizsardzības darba grupai 12 mēnešu laikā pēc šā ieteikuma publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī*.

5. Dalībvalstīm vajadzētu nodrošināt, ka operatori, neskarot to pienākumus, kas noteikti Direktīvā 95/46/EK, īsteno šādas darbības:

a) sagatavo novērtējumu par to, kā lietojuma īstenošana ietekmēs personas datu un privātuma aizsardzību, tostarp par to, vai lietojumu varētu izmantot privātpersonu uzraudzībai. Novērtējuma detalizācijas līmenim vajadzētu atbilst tam, cik lielā mērā konkrētais lietojums varētu apdraudēt privātumu;

b) īsteno pienācīgus tehniskus un organizatoriskus pasākumus, lai nodrošinātu personas datu un privātuma aizsardzību;

c) ieceļ personu vai personu grupu, kas atbildīgas par novērtējumu un tehnisko un organizatorisko pasākumu turpmākas piemērotības pārskatīšanu, lai nodrošinātu personas datu un privātuma aizsardzību;

d) novērtējumu dara pieejamu kompetentajai iestādei vismaz sešas nedēļas pirms lietojuma ieviešanas;

e) kad ir pieejams 4. punktā aprakstītais privātuma un datu aizsardzības ietekmes novērtējums, īsteno iepriekš minētos noteikumus saskaņā ar to.

Informācijas drošība

6. Dalībvalstīm vajadzētu palīdzēt Komisijai noteikt, kādi ir tie lietojumi, kas varētu radīt informācijas drošības apdraudējumus, kuri skar sabiedrību kopumā. Attiecībā uz šādiem lietojumiem dalībvalstīm vajadzētu nodrošināt, ka operatori kopā ar valstu kompetentajām iestādēm un pilsoniskās sabiedrības organizācijām izstrādā jaunas vai piemēro jau esošās shēmas, piemēram, sertificēšanu vai operatoru pašnovērtējumu, lai pierādītu, ka attiecībā uz novērtētajiem riskiem ir izveidots pienācīgs informācijas drošības un privātuma aizsardzības līmenis.

Informācija un RFID izmantošanas pārredzamība

7. Neskarot par datu apstrādi atbildīgo personu pienākumus, kas noteikti Direktīvā 95/46/EK un Direktīvā 2002/58/EK, dalībvalstīm būtu jānodrošina, ka operatori sagatavo un publicē īsu, precīzu un viegli saprotamu informācijas kopsavilkumu par katru savu lietojumu. Minētajā dokumentā iekļaujama vismaz šāda informācija:

a) operatoru identitāte un adrese;

b) lietojuma mērķis;

c) kādus datus šajā lietojumā apstrādās, jo īpaši, ja tiks apstrādāti personas dati, kā arī – vai tiks veikta uzraudzīta, lai sekotu marķējuma atrašanās vietai;

d) privātuma un datu aizsardzības ietekmes novērtējuma kopsavilkums;

e) iespējamie ar privātumu saistītie riski (ja tādi ir) saistībā ar marķējuma izmantošanu lietojumā un pasākumi, kurus personas var īstenot šo risku mazināšanai.

8. Izmantojot visā Eiropā kopēju apzīmējumu, ko izstrādājušas Eiropas standartizācijas organizācijas ar attiecīgo ieinteresēto personu atbalstu, dalībvalstīm vajadzētu nodrošināt, ka operatori īsteno pasākumus, lai iedzīvotājus informētu par lasītāju esamību. Uz šā apzīmējuma vajadzētu norādīt arī operatora identifikācijas datus un kontaktpersonu, lai iedzīvotāji varētu saņemt lietojuma informācijas politiku.

RFID lietojumi mazumtirdzniecībā

9. Izmantojot visā Eiropā kopēju apzīmējumu, ko izstrādājušas Eiropas standartizācijas organizācijas ar attiecīgo ieinteresēto personu atbalstu, operatoriem vajadzētu informēt iedzīvotājus par uz izstrādājumiem izvietotām vai tajos iestrādātu marķējumu.

10. Veicot privātuma un datu aizsardzības ietekmes novērtējumu, kā aprakstīts 4. un 5. punktā, lietojuma operatoram būtu īpaši jāizvērtē, vai marķējums, kas izvietots uz tādiem izstrādājumiem vai iestrādāts tādos izstrādājumos, kurus patērētājiem pārdod mazumtirgotāji, kas nav konkrētā lietojuma operatori, nevar radīt draudus privātumam vai personas datu aizsardzībai.

11. Mazumtirgotājiem savos lietojumos izmantotais marķējums būtu jādeaktivē vai jānoņem tirdzniecības vietā, izņemot, ja patērētāji pēc tam, kad viņi ir informēti par 7. punktā aprakstīto politiku, piekrīt, ka marķējumu nedeaktivē. Ar marķējuma deaktivāciju būtu jāsaprot jebkurš tāds process, ar kuru pārtrauc marķējuma mijiedarbību ar vidi un kura īstenošanai nav nepieciešama patērētāja aktīva līdzdalība. Mazumtirgotājam marķējumu vajadzētu deaktivēt vai noņemt nekavējoties un bez maksas. Patērētājiem vajadzētu būt iespējai pārliecināties, ka deaktivācija vai noņemšana ir notikusi.

12. Šā ieteikuma 11. punktu nevajadzētu piemērot, ja privātuma un datu aizsardzības ietekmes novērtējumā secināts, ka marķējums, kas izmantots mazumtirdzniecības lietojumam un saglabā darbspēju ārpus tirdzniecības vietas, nerada iespējamu privātuma vai personas datu aizsardzības apdraudējumu. Tomēr mazumtirgotājiem vajadzētu bez maksas darīt pieejamus vienkāršus līdzekļus, ar kuriem nekavējoties vai vēlāk minēto marķējumu var noņemt.

13. Marķējuma deaktivēšana vai noņemšana nedrīkstētu būt saistīta ne ar kādu mazumtirgotāja vai ražotāja juridisko saistību pret patērētāju ierobežošanu vai pārtraukšanu.

14. Šā ieteikuma 11. un 12. punktam būtu jāattiecas tikai uz tiem operatoriem, kas ir mazumtirgotāji.

Izpratnes padziļināšanas pasākumi

15. Dalībvalstīm sadarbībā ar nozari, Komisiju un citām ieinteresētajām personām vajadzētu veikt piemērotus pasākumus, lai informētu un padziļinātu iestāžu un uzņēmumu, jo īpaši MVU, izpratni par potenciālajiem ieguvumiem un risku, kas saistīts ar *RFID* tehnoloģijas izmantošanu. Īpaša uzmanība būtu jāpievērš informācijas drošības un privātuma aspektiem.

16. Dalībvalstīm sadarbībā ar nozari, pilsoniskās sabiedrības apvienībām, Komisiju un citām ieinteresētajām personām vajadzētu noteikt un sniegt labas prakses piemērus par *RFID* lietojumu ieviešanu, lai informētu par tiem sabiedrību un padziļinātu tās izpratni par šo jomu. Dalībvalstīm vajadzētu arī veikt piemērotus pasākumus, piemēram, liela mēroga izmēģinājuma projektus, lai veicinātu sabiedrības izpratni par *RFID* tehnoloģiju, tās priekšrocībām, radīto risku un lietošanas īpatnībām, kas palīdzētu plašāk ieviest šo tehnoloģiju.

Pētniecība un attīstība

17. Dalībvalstīm būtu jāsadarbojas ar nozari, attiecīgām pilsoniskās sabiedrības ieinteresētajām personām un Komisiju, lai, jau sākot ar agrīnu *RFID* lietojumu izstrādāšanas posmu, veicinātu un atbalstītu "integrētas drošības un privātuma aizsardzības" principu.

Turpmākie pasākumi

18. Dalībvalstīm vajadzētu veikt visus vajadzīgos pasākumus, lai ar šo ieteikumu iepazītos visas ieinteresētās personas, kas Kopienā iesaistītas *RFID* lietojumu projektēšanā un ekspluatācijā.

19. Dalībvalstis vēlākais 24 mēnešus pēc šā ieteikuma publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī* informē Komisiju par saistībā ar šo ieteikumu veiktajiem pasākumiem.

20. Trīs gadu laikā pēc šā ieteikuma publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī* Komisija sagatavo ziņojumu par šā ieteikuma īstenošanu, efektivitāti un ietekmi uz operatoriem un patērētājiem, jo īpaši attiecībā uz 9. līdz 14. punktā iekļautajiem ieteikumiem.

Adresāti

21. Šis ieteikums ir adresēts dalībvalstīm.

Briselē, 2009. gada 12. maijā

Komisijas vārdā —
Komisijas locekle
Viviane REDING