# AJÁNLÁSOK

# BIZOTTSÁG

## A BIZOTTSÁG AJÁNLÁSA

**(2009. május 12.)**

**a magánélet- és adatvédelmi alapelveknek a rádiófrekvenciás azonosítás által támogatott alkalmazások területén történő alkalmazásáról**

*(az értesítés a C(2009) 3200. számú dokumentummal történt)*

(2009/387/EK)

AZ EURÓPAI KÖZÖSSÉGEK BIZOTTSÁGA,

tekintettel az Európai Közösséget létrehozó szerződésre és különösen annak 211. cikkére,

az európai adatvédelmi biztossal folytatott konzultációt követően,

mivel:

(1) A rádiófrekvenciás azonosítás (RFID) az információs társadalomnak egy olyan új fejlesztését jelenti, amellyel az automatikus adatfeldolgozásra képes mikroelektronikával felszerelt eszközök egyre inkább a mindennapi élet szerves részévé válhatnak.

(2) Az RFID egyre gyorsabban terjed és válik az egyének életének részévé olyan különféle alkalmazási területeken, mint a logisztika ([1]), az egészségügy, a tömegközlekedés, a kiskereskedelem, különösen a termékbiztonság javítása és a gyorsabb termékvisszavonások területén, a szórakozás, a munka, az útdíjszedés, a poggyászkezelés és az úti okmányok.

(3) Az RFID-technológia a benne rejlő lehetőségek révén a növekedés és a munkahelyteremtés új motorjává válhat, és így jelentős szerepet játszhat a lisszaboni stratégia megvalósításában, mivel gazdasági szempontból igen ígéretes tulajdonságaival új üzleti lehetőségeket teremthet, költségcsökkentő és hatékonyságnövelő hatást gyakorolhat, különösen a hamisítások visszaszorítása, az e-hulladék és veszélyes anyagok kezelése, valamint az elhasználódott termékek újrahasznosítása területén.

(4) Az RFID-technológia rövid távolságok között lehetővé teszi a címke leolvasója vagy írója, valamint a címke közötti bármilyen fizikai kapcsolat vagy látható kölcsönhatás nélkül az adatfeldolgozást, beleértve a személyes adatokat is, oly módon, hogy e kölcsönhatás az érintett egyén tudomása nélkül is végbemehet.

(5) Az RFID-alkalmazások lehetőséget nyújtanak egy azonosított vagy azonosítható természetes személlyel, egy közvetve vagy közvetlenül éppen azonosítandó természetes személlyel kapcsolatos adatok feldolgozására. Képesek feldolgozni a címkén tárolt olyan személyes adatokat, mint például a személy neve, születési ideje, lakhelye vagy biometrikus adatai, illetve az olyan adatokat, amelyek a meghatározott RFID-tételszámot összekötik a rendszer másik részében tárolt személyes adatokkal. Ezen alkalmazandó technológia lehetőséget biztosít továbbá olyan egyének nyomon követésére, akiknek a tulajdonában RFID-tételszámot tartalmazó egy vagy több tétel van.

(6) Mivel fennáll a lehetőség, hogy az RFID széles körben elterjed, és gyakorlatilag láthatatlanná válik, az RFID fejlesztése során különös figyelmet kell fordítani az adatvédelemmel és a magánélet védelmével kapcsolatos kérdésekre. Következésképpen a magánélet védelmét és az információbiztonságot még a széles körű elterjedésüket megelőzően be kell építeni az RFID-alkalmazásokba („beépített biztonság és magánélet-védelem” elve).

(7) Az RFID csak akkor váltja valóra a benne rejlő számos gazdasági és társadalmi előnyt, ha hatékony garanciák állnak rendelkezésre az RFID nyilvános elfogadásáról folytatott vita központjában álló adatvédelemre, a magánélet biztonságára és a kapcsolódó etikai szempontokra vonatkozóan.

(8) A tagállamoknak és az érdekelt feleknek – különösen az RFID bevezetésének e kezdeti szakaszában – további erőfeszítéseket kell tenniük annak érdekében, hogy biztosítsák az RFID-alkalmazások nyomon követését és az egyének jogainak és szabadságainak tiszteletben tartását.

([1]) COM(2007) 607 végleges.

(9) A „Rádiófrekvenciás azonosítás (RFID) Európában: lépések egy politikai keret felé" című, 2007. március 15-i közleményében [1] a Bizottság bejelentette, hogy egy vagy több bizottsági ajánlásban tisztázzák a feltételeket, és iránymutatást nyújtanak az RFID-alkalmazások adatvédelmi és a magánélet védelmére vonatkozó aspektusaihoz.

(10) A személyes adatok védelmével és az ilyen adatok szabad mozgásával kapcsolatos jogok és kötelességek, amelyeket a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló, 1995. október 24-i 95/46/EK európai parlamenti és a tanácsi irányelv [2], valamint az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló, 2002. július 12-i 2002/58/EK európai parlamenti és tanácsi irányelv (elektronikus hírközlési adatvédelmi irányelv) [3] előír, teljes mértékben alkalmazandók a személyes adatokat feldolgozó RFID-alkalmazások használata során.

(11) Az RFID-alkalmazások fejlesztésénél a rádióberendezésekről és a távközlő végberendezésekről, valamint a megfelelőségük kölcsönös elismeréséről szóló, 1999. március 9-i 1999/5/EK európai parlamenti és tanácsi irányelvben [4] meghatározott elveket kell alkalmazni.

(12) Az európai adatvédelmi biztos véleménye [5] iránymutatást nyújt az egyének számára hozzáférhető és címkéket tartalmazó termékek kezelési módjára vonatkozóan, valamint felszólít a magánélet védelmére és a biztonságra vonatkozó hatásvizsgálatok elvégzésére az elérhető legjobb technikák azonosítása és fejlesztése érdekében, hogy így garantálják az RFID-rendszerekben a magánélet védelmét és a biztonságot.

(13) Az RFID-alkalmazás üzemeltetői minden ésszerű lépést megtesznek annak biztosítására, hogy sem az RFID-alkalmazás kezelője, sem bármely más személy által valószínűsíthetően felhasználható semmilyen eszközzel ne legyenek összekapcsolhatók az adatok egy azonosítható vagy már azonosított személlyel, kivéve, ha az adatok feldolgozása az alkalmazandó elvekkel és az adatvédelemre vonatkozó jogszabályokkal összhangban történik.

(14) Az adatvédelemnek a magánélet védelmét erősítő technológiák által történő ösztönzéséről szóló, 2007. május 2-i bizottsági közlemény [6] egyértelmű intézkedéseket határoz meg annak elérése érdekében, hogy a magánélet védelmét elősegítő technológiák fejlesztésével, valamint azok adatkezelők és egyének által történő alkalmazásával a személyes adatok kezelése minimális mértékű legyen, és hogy amikor csak lehet, anonim vagy álnéven szereplő adatok használatára kerüljön sor.

(15) „A biztonságos információs társadalomra irányuló stratégia: párbeszéd, partnerség, felvértezés és felelősségvállalás" című, 2006. március 31-i közleményében [7] a Bizottság elismeri, hogy a sokszínűség, a nyitottság, a kölcsönös átjárhatóság, a felhasználhatóság és a verseny a biztonságos információs társadalom legfőbb motorjai, kiemeli a tagállamoknak és a közigazgatásnak a tájékoztatásban és a helyes biztonsági gyakorlatok elterjesztésében betöltött szerepét, valamint felkéri a magánszektor érdekelt szereplőit, hogy tegyenek kezdeményezéseket a kimondottan EU-igényeknek (különösen a személyes adatok védelme terén) megfelelő termékekre, szolgáltatásokra és folyamatokra vonatkozó, széles körben elérhető tanúsítási rendszerek létrehozására.

(16) A biztonságos európai információs társadalomra irányuló stratégiáról szóló, 2007. március 22-i állásfoglalásában [8] a Tanács felkérte a tagállamokat, hogy fordítsanak kellő figyelmet az elektronikus kommunikációs hálózatokra leselkedő új és már meglévő veszélyek megelőzésének és az ellenük való küzdelemnek a szükségességére.

(17) A magánélet védelméről és adatvédelemről készített hatásvizsgálat lefolytatására megteremtett közösségi szintű keret fogja biztosítani ezen ajánlás rendelkezéseinek a tagállamokban történő következetes betartását. Az ilyen keret kialakítását a meglévő gyakorlatra és a tagállamokban, harmadik országokban nyert tapasztalatokra, valamint az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) [9] által folytatott munkára szükséges alapozni.

(18) A Bizottság a meglévő gyakorlatra és a tagállamokban, harmadik országokban nyert tapasztalatokra építve biztosítja az RFID-alkalmazások információbiztonsági szempontból történő irányítására vonatkozó közösségi szintű iránymutatások kidolgozását. A tagállamoknak is hozzá szükséges járulniuk e folyamatokhoz, és ösztönözniük szükséges a magánjogi szervezetek, valamint az állami szervek részvételét.

(19) Az RFID-alkalmazások végrehajtását megelőzően az üzemeltető által a magánélet védelméről és adatvédelemről készített hatásvizsgálat fogja biztosítani a kívánt információt a megfelelő védőintézkedésekhez. Az RFID-alkalmazás élettartama alatt szükség van az ilyen intézkedések nyomon követésére és felülvizsgálatára.

(20) A kiskereskedelmi ágazatban a fogyasztóknak árusított, címkével ellátott termékeknek a magánélet védelmére és adatvédelemre gyakorolt hatásairól készített vizsgálatnak kell a szükséges adatokkal szolgálnia annak eldöntéséhez, hogy fennáll-e a magánélet védelmének, illetve a személyes adatok védelmének valószínűsíthető fenyegetettsége.

[1] COM(2007) 96 végleges.
[2] HL L 281., 1995.11.23., 31. o.
[3] HL L 201., 2002.7.31., 37. o.
[4] HL L 91., 1999.4.7., 10. o.
[5] HL C 101., 2008.4.23., 1. o.
[6] COM(2007) 228 végleges.
[7] COM(2006) 251 végleges.
[8] HL C 68., 2007.3.24., 1. o.
[9] A 460/2004/EK európai parlamenti és tanácsi rendelet (HL L 77., 2004.3.13., 1. o.) 2. cikkének (1) bekezdése.

(21) Az RFID-alapú üzleti folyamatok során a nemzetközi szabványok – pl. amelyeket a Nemzetközi Szabványügyi Szervezet (ISO) dolgozott ki –, eljárási szabályok, valamint az EU keretszabályozásának megfelelő legjobb módszerek használata segíthet az információbiztonság és a magánélet védelme területén hozott intézkedések lebonyolításában.

(22) A lakosságra is kiható RFID-alkalmazások, mint pl. a tömegközlekedésben alkalmazott elektronikus jegyek, megfelelő védőintézkedéseket igényelnek. Információbiztonsági szempontból különösen kényes területet képeznek, ennélfogva külön figyelmet érdemelnek azok az RFID-alkalmazások, amelyek például a biometrikus azonosító adatok, vagy egészségügyi adatok feldolgozása révén érintik az egyéneket.

(23) Fontos, hogy a társadalom egésze tudatában legyen az RFID-alkalmazások használatához kapcsolódó jogoknak és kötelességnek. A technológiát kiépítő felek feladata tehát, hogy az egyéneket tájékoztassák ezen alkalmazások felhasználási módjáról.

(24) Az állami, valamint a kis- és középvállalkozások (kkv-k) figyelmének felkeltése az RFID tulajdonságai és a benne rejlő képességek iránt segíthet abban, hogy e technológia valóra váltsa a benne rejlő gazdasági lehetőségeket, csökkentve ugyanakkor a közérdek kárára történő felhasználásának kockázatát, így fokozva annak elfogadottságát.

(25) A Bizottság az érdekelt felek közötti párbeszéd és együttműködés előmozdításával közvetlenül és közvetve is hozzájárul ezen ajánlás végrehajtásához, különösen az 1639/2006/EK európai parlamenti és tanácsi határozatban [1] létrehozott versenyképességi és innovációs keretprogramon (CIP), valamint az 1982/2006/EK európai parlamenti és tanácsi határozattal [2] létrehozott hetedik (FP7) keretprogramon keresztül.

(26) A magánélet védelmét fokozó alacsony költségű technológiákra és az információbiztonsági technológiákra irányuló kutatás és fejlesztés fontos szerepet játszik e technológiák széleskörű átvételének közösségi szinten történő megfelelő előmozdításában.

(27) Ez az ajánlás tiszteletben tartja az alapvető jogokat, és figyelembe veszi különösen az Európai Unió alapjogi chartája által elismert alapelveket. Ennek az ajánlásnak célja különösképpen, hogy biztosítsa a magán- és családi élet teljes tiszteletben tartását, valamint a személyes adatok védelmét,

[1] HL L 310., 2006.11.9., 15. o.
[2] HL L 412., 2006.12.30., 1. o.

AJÁNLJA:

**Hatály**

1. Ez az ajánlás iránymutatást nyújt a tagállamoknak az RFID-alkalmazások jogszerű, etikailag, társadalmilag és politikailag is elfogadható tervezéséhez és üzemeltetéséhez a magánélet védelméhez való jog, valamint a személyes adatok védelmének biztosítása mellett.

2. Ez az ajánlás iránymutatást nyújt az RFID-alkalmazások üzembe helyezésénél szükséges intézkedésekre vonatkozóan annak érdekében, hogy a 95/46/EK, az 1999/5/EK és a 2002/58/EK irányelvet végrehajtó nemzeti jogszabályok tiszteletben tartása az ilyen alkalmazások bevezetése során adott esetben biztosítva legyen.

**Fogalommeghatározások**

3. Ennek az ajánlásnak az alkalmazásában a 95/46/EK irányelvben megállapított fogalommeghatározásokat kell alkalmazni. A következő meghatározásokat ugyancsak alkalmazni kell:

a) „rádiófrekvenciás azonosítás” (RFID): az elektromágneses hullámok, illetve elektromágneses mező segítségével a rádiófrekvencia-spektrum megfelelő tartományában létrejövő kapcsolat egy címkével számos modulációs és kódrendszeren keresztül folytatott kommunikáció lebonyolítására annak érdekében, hogy egy rádiófrekvenciás címke azonosítóját, illetve a címkén tárolt egyéb adatokat egyedileg leolvassák;

b) „RFID-címke” vagy „címke”: rádiójelet kibocsátani képes RFID-berendezés, vagy az olvasó/író által kibocsátott vivőjelet (a készülék típusától függően) vevő, visszasugárzó, illetve visszaverő, valamint azt moduláló berendezés;

c) „RFID-olvasó vagy -író”, illetve „olvasó”: egy rögzített vagy mobil adatdigitalizáló és -azonosító berendezés, amely rádiófrekvenciás elektromágneses hullámok vagy térerőcsatolás segítségével címkéből vagy címkék egy csoportjából módosított válaszjeleket vált ki, valamint érzékeli és azonosítja azokat;

d) „RFID-alkalmazás”, illetve „alkalmazás”: az a címkék és leolvasók használatával történő adatfeldolgozási folyamat, amelyet háttérrendszer és globális hálózati kommunikációs infrastruktúra támogat;

e) „RFID-alkalmazás üzemeltetője” vagy „üzemeltető”: az a természetes, vagy jogi személy, hatóság, intézmény vagy bármely más szerv, amely önállóan vagy másokkal együtt meghatározza az alkalmazás üzemeltetésének céljait és módját, beleértve az RFID-alkalmazást felhasználó személyes adatainak kezelőjét is;

f) „információbiztonság”: az adatok titkosságának, sértetlenségének és rendelkezésre állásának megőrzése;

g) „nyomon követés”: bármely tevékenység, amely egy személy hollétének, mozgásának, tevékenységeinek vagy állapotának megállapítására, megfigyelésére, másolására vagy rögzítésére irányul.

**A magánélet védelméről és adatvédelemről készített hatásvizsgálat**

4. A tagállamoknak biztosítaniuk szükséges, hogy az ágazat a civil társadalom érintett szereplőivel együttműködve kialakítsa a magánélet védelmére és adatvédelemre irányuló hatásvizsgálat kereteit. E keretet az *Európai Unió Hivatalos Lapjában* való kihirdetését követő tizenkét hónapon belül szükséges jóváhagyásra beterjeszteni a 29. cikk alapján létrehozott adatvédelmi munkacsoporthoz.

5. A tagállamoknak biztosítaniuk szükséges, hogy az üzemeltetők, a 95/46/EK irányelv szerinti egyéb kötelezettségeiktől függetlenül:

a) értékelést végezzenek arra vonatkozóan, hogy az alkalmazás végrehajtása milyen hatással lesz a személyes adatok és a magánélet védelmére, beleértve azt is, hogy az alkalmazás felhasználható-e egy személy nyomon követésére. Az értékelésnek olyan részletességűnek szükséges lennie, amely megfelel az alkalmazás felhasználásával várhatóan felmerülő, a magánélet védelmével kapcsolatos kockázatoknak;

b) megfelelő műszaki és szervezeti intézkedéseket tegyenek a személyes adatok és a magánélet védelmének biztosítása érdekében;

c) kinevezzék az értékelésnek, valamint a műszaki és szervezeti intézkedések további megfelelőségének felülvizsgálatáért felelős személyt vagy csoportot a személyes adatok és a magánélet védelmének biztosítása érdekében;

d) legalább hat héttel az alkalmazás üzembe helyezése előtt hozzáférhetővé tegyék az értékelést az illetékes hatóság számára;

e) mihelyst rendelkezésre állnak a magánélet védelmére és adatvédelemre irányuló hatásvizsgálatnak a 4. pontban előírt keretei, azoknak megfelelően végrehajtják a fenti intézkedéseket.

**Információbiztonság**

6. A tagállamoknak támogatniuk kell a Bizottságot az olyan információbiztonsági kockázatokat magukban rejtő alkalmazások azonosításában, amelyek a lakosságra nézve következményekkel járnak. A tagállamoknak biztosítaniuk kell, hogy az üzemeltetők az illetékes nemzeti hatóságokkal és a civil társadalmi szervezetekkel együtt új rendszereket hozzanak létre, vagy olyan már létező rendszereket alkalmazzanak, mint az igazolás vagy önértékelés, annak bizonyítására, hogy a vizsgált veszélyekkel kapcsolatban kiépült az információbiztonságnak és a magánélet védelmének a megfelelő szintje.

**Az RFID használatához kapcsolódó tájékoztatás és átláthatóság**

7. Az adatkezelőkre vonatkozó kötelezettségek sérelme nélkül, a 95/46/EK és 2002/58/EK irányelvvel összhangban a tagállamoknak gondoskodniuk kell arról, hogy az üzemeltetők minden egyes alkalmazásukra vonatkozóan tömör, pontos és könnyen érthető tájékoztatási politikát dolgozzanak ki és tegyenek közzé. A politikának legalább az alábbiakat szükséges tartalmaznia:

a) az üzemeltető személyazonossága és címe;

b) az alkalmazás célja;

c) az alkalmazás által feldolgozásra kerülő adatok típusa, különösen, hogy személyes adatok is feldolgozásra kerülnek-e, és hogy a címkék hollétét nyomon fogják-e követni;

d) a magánélet védelméről és adatvédelemről készített hatásvizsgálat összefoglalása;

e) az alkalmazásnál használt címkékkel kapcsolatban valószínűleg felmerülő magánélet-védelmi kockázatok, ha vannak ilyenek, valamint hogy mit tehet az egyén e kockázatok csökkentése érdekében.

8. A tagállamoknak biztosítaniuk szükséges, hogy az üzemeltetők az európai szabványosítási szervezetek által és az érintett érdekeltek támogatásával létrehozott közös európai jelzés alapján tájékoztassák az egyéneket a leolvasók jelenlétéről. A jelzésnek tartalmaznia szükséges az üzemeltető személyazonosságát, valamint az egyének számára létrehozott kapcsolattartási pontot, ahol megismerhetik az alkalmazáshoz kapcsolódó tájékoztatási politikát.

**Az RFID-alkalmazások kiskereskedelemben történő felhasználása**

9. Az európai szabványosítási szervezetek által és az érintett érdekeltek támogatásával létrehozott közös európai jelzés alapján az üzemeltetőknek tájékoztatniuk szükséges az egyéneket a termékekre vagy termékekbe helyezett címkék jelenlétéről.

10. A 4. és 5. pontban említett, a magánélet védelméről és adatvédelemről készített hatásvizsgálat lefolytatása során az alkalmazás üzemeltetőjének szükséges meghatároznia, hogy a magánélet és a személyes adatok védelmére nézve valószínű veszélyt képviselnek-e az olyan termékekre, illetve termékekbe helyezett címkék, amelyek esetében a fogyasztóknak értékesítő kiskereskedők az adott alkalmazásnak nem üzemeltetői.

11. A kiskereskedőknek az árusítás helyén hatástalanítaniuk szükséges vagy el kell távolítaniuk az általuk használt alkalmazás címkéit, kivéve, ha a fogyasztók hozzájárulásukat adják a címkék üzemben tartásához, miután tájékoztatták őket a 7. pontban említett politikáról. A címkék hatástalanításán azt az eljárást kell érteni, amely megakadályozza a címke és a környezete közötti olyan kölcsönhatásokat, amelyekhez nem szükséges a fogyasztó aktív közreműködése. A címkék hatástalanítását vagy eltávolítását a kiskereskedőnek haladéktalanul és díjtalanul szükséges elvégeznie a fogyasztó számára. A fogyasztók számára lehetővé szükséges tenni a hatástalanítás, illetve eltávolítás eredményességének ellenőrzését.

12. A 11. pontot nem indokolt alkalmazni abban az esetben, ha a magánélet védelméről és adatvédelemről készített hatásvizsgálat arra a megállapításra jut, hogy nem képviselnek valószínű veszélyt a magánélet és a személyes adatok védelmére nézve azok a címkék, amelyeket az alkalmazás kiskereskedelemben történő felhasználása során használnak, és üzemben maradnak az árusítóhely elhagyását követően is. A kiskereskedőknek mindazonáltal lehetővé kell tenniük, hogy e címkék díjtalanul és könnyedén, azonnal vagy egy későbbi időpontban hatástalaníthatók vagy eltávolíthatók legyenek.

13. A címkék hatástalanítása vagy eltávolítása nem járhat a kiskereskedők vagy gyártók fogyasztókkal szemben fennálló jogi kötelezettségeinek semmiféle csökkenésével, illetve megszűnésével.

14. A 11. és 12. pontot csak azoknak a kiskereskedőknek szükséges alkalmazniuk, akik egyben üzemeltetők is.

**Figyelemfelkeltő intézkedések**

15. A tagállamoknak az ágazattal, a Bizottsággal és más érdekelt felekkel együttműködve megfelelő intézkedéseket szükséges tenniük ahhoz, hogy tájékoztassák és felvilágosítsák a hatóságokat és a vállalatokat, különösen a kkv-kat, az RFID-technológiához kapcsolódó lehetséges előnyökről és kockázatokról. A biztonsággal és a magánélet védelmével kapcsolatos kérdésekre különös figyelmet szükséges fordítani.

16. A lakosság tájékoztatása és figyelmének felkeltése érdekében a tagállamoknak az iparággal, a civil társadalmi szervezetekkel, a Bizottsággal és az egyéb érintett felekkel együttműködve fel szükséges ismerniük, és be szükséges mutatniuk a helyes gyakorlati megoldásokat az RFID-alkalmazások végrehajtása területén. E technológia széles körű átvételének előfeltételeként a tagállamoknak megfelelő intézkedéseket szükséges tenniük például nagyszabású kísérleti programok révén, hogy növeljék a közvéleménynek az RFID technológiával kapcsolatos tájékozottságát.

**Kutatás és fejlesztés**

17. A tagállamoknak már az RFID-alkalmazások fejlesztésének korai szakaszában együtt szükséges működniük az iparral, a civil társadalom érintett szereplőivel, és a Bizottsággal a „beépített biztonság és magánélet-védelem” elve bevezetésének ösztönzésében és támogatásában.

**Nyomon követés**

18. A tagállamoknak minden, a Közösségen belül RFID-alkalmazások tervezésében és üzemeltetésében érdekelt fél tájékoztatásához szükséges intézkedést meg indokolt tenniük.

19. A tagállamok legkésőbb huszonnégy hónappal ezen ajánlásnak az *Európai Unió Hivatalos Lapjában* történő kihirdetését követően tájékoztatják a Bizottságot az ajánlás nyomán végrehajtott intézkedéseikről.

20. Három évvel ezen ajánlásnak az *Európai Unió Hivatalos Lapjában* történő kihirdetését követően a Bizottság jelentést tesz ezen ajánlás végrehajtásáról, annak hatékonyságáról, valamint az üzemeltetőkre és fogyasztóra gyakorolt hatásáról, különösen a 9. és 14. pontban javasoltakat illetően.

**Címzettek**

21. Ennek az ajánlásnak a tagállamok a címzettjei.

Kelt Brüsszelben, 2009. május 12-én.

*a Bizottság részéről*

Viviane REDING

*a Bizottság tagja*