ODPORÚČANIA

KOMISIA

ODPORÚČANIE KOMISIE

z 12. mája 2009

o vykonávaní zásad ochrany súkromia a údajov v aplikáciách podporovaných rádiofrekvenčnou identifikáciou

[oznámené pod číslom K(2009) 3200]

(2009/387/ES)

KOMISIA EURÓPSKYCH SPOLOČENSTIEV,

so zreteľom na Zmluvu o založení Európskeho spoločenstva, a najmä na jej článok 211,

po porade s európskym dozorným úradníkom pre ochranu údajov,

keďže:

(1) Rádiofrekvenčná identifikácia (RFID) znamená nový vývoj v informačnej spoločnosti, v ktorej sa zariadenia vybavené mikroelektronikou, ktorá dokáže spracovať údaje automaticky, budú čoraz viac stávať neoddeliteľnou súčasťou každodenného života.

(2) RFID sa postupne stáva bežnejšia, a teda súčasťou života jednotlivcov v rôznych oblastiach, medzi ktoré patrí logistika [1], zdravotná starostlivosť, verejná doprava, maloobchod, najmä pre zlepšenú bezpečnosť výrobkov a rýchlejšie spätné prevzatie výrobkov, zábava, práca, správa cestného mýta, správa batožiny a cestovné doklady.

(3) Technológia RFID má potenciál stať sa novým motorom rastu a zamestnanosti, a tým výrazne prispieva k lisabonskej stratégii, pretože je z hospodárskeho hľadiska veľkým prísľubom, keďže môže priniesť nové podnikateľské príležitosti, znížiť náklady a zvýšiť účinnosť najmä v boji proti falšovaniu a v správe elektronického odpadu, nebezpečných materiálov a v recyklovaní výrobkov na konci ich životnosti.

(4) Technológia RFID umožňuje spracovať údaje vrátane osobných údajov na krátke vzdialenosti bez fyzického kontaktu alebo viditeľnej interakcie medzi čítačkou alebo zapisovačkou a štítkom, takže táto interakcia sa môže uskutočniť bez toho, aby o tom vedel dotknutý jednotlivec.

(5) Aplikácie RFID majú potenciál spracovať údaje týkajúce sa identifikovaných alebo identifikovateľných fyzických osôb, pričom fyzická osoba sa identifikuje priamo alebo nepriamo. Dokážu spracovať osobné údaje uchované na štítku, napríklad meno osoby, dátum narodenia alebo adresu, alebo biometrické údaje alebo údaje spájajúce číslo osobitnej položky RFID s osobnými údajmi uloženými niekde inde v systéme. Okrem toho existuje možnosť použitia tejto technológie na monitorovanie jednotlivcov prostredníctvom toho, že vlastnia jednu alebo viac položiek, ktoré obsahujú číslo položky RFID.

(6) V dôsledku toho, že RFID má potenciál byť všadeprítomná a súčasne prakticky neviditeľná, je pri jej zavedení potrebné venovať osobitnú pozornosť otázkam ochrany súkromia a údajov. V dôsledku toho by sa vlastnosti bezpečnosti súkromia a informácií mali zabudovať do aplikácií RFID pred ich širokým využívaním (zásada „bezpečnosti a prihliadania na ochranu súkromia už od návrhu“).

(7) RFID dokáže so sebou priniesť mnohé hospodárske a spoločenské výhody iba vtedy, ak sa zavedú účinné opatrenia na zabezpečenie ochrany osobných údajov, súkromia a súvisiacich etických zásad, ktoré tvoria základ diskusie o uznaní RFID verejnosťou.

(8) Členské štáty a zainteresované strany by najmä v tejto počiatočnej fáze realizácie RFID mali vyvinúť ďalšie úsilie na zabezpečenie, aby sa aplikácie RFID monitorovali a aby sa dodržiavali práva a slobody jednotlivcov.

[1] KOM(2007) 607 v konečnom znení.

(9) Komisia vo svojom oznámení z 15. marca 2007 s názvom Rádiofrekvenčná identifikácia (RFID) v Európe: kroky k politickému rámcu [1] oznámila, že prostredníctvom jedného alebo viacerých odporúčaní Komisie sa poskytne objasnenie a usmernenie týkajúce sa aspektov ochrany údajov a súkromia v aplikáciách RFID.

(10) Práva a povinnosti týkajúce sa ochrany osobných údajov a voľného pohybu takýchto údajov, ustanovené v smernici Európskeho parlamentu a Rady 95/46/ES z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov [2] a smernici Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002 týkajúcej sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách) [3], sa v plnej miere vzťahujú na používanie aplikácií RFID, ktoré spracúvajú osobné údaje.

(11) Zásady ustanovené v smernici Európskeho parlamentu a Rady 1999/5/ES z 9. marca 1999 o rádiovom zariadení a koncových telekomunikačných zariadeniach a o vzájomnom uznávaní ich zhody [4] by sa mali uplatňovať pri vývoji aplikácií RFID.

(12) V stanovisku európskeho dozorného úradníka pre ochranu údajov [5] sa poskytuje usmernenie k spôsobu, ako zaobchádzať s výrobkami, ktoré obsahujú štítky, ktoré sa poskytujú jednotlivcom, a vyzýva, aby sa v posúdeniach vplyvu na súkromie a bezpečnosť údajov určili a vypracovali „najlepšie dostupné metódy“ na zabezpečenie súkromia a bezpečnosti systémov RFID.

(13) Prevádzkovatelia aplikácií RFID by mali prijať všetky primerané opatrenia zabezpečujúce, aby sa údaje netýkali identifikovanej alebo identifikovateľnej fyzickej osoby prostredníctvom akýchkoľvek prostriedkov, v prípade ktorých je pravdepodobné, že ich použije buď prevádzkovateľ aplikácie RFID, alebo akákoľvek iná osoba, pokiaľ sa takéto údaje nespracujú v súlade s platnými zásadami a právnymi predpismi o ochrane údajov.

(14) V oznámení Komisie z 2. mája 2007 o „podpore ochrany údajov prostredníctvom technológií na zvyšovanie ochrany súkromia (PET)“ [6] sú ustanovené jasné opatrenia na dosiahnutie cieľa, ktorým je minimalizovať spracovanie osobných údajov a používanie anonymných alebo pseudonymných údajov vždy, keď je to možné prostredníctvom vývoja PET a ich používania správcom údajov a jednotlivcami.

(15) V oznámení Komisie z 31. mája 2006 s názvom Stratégia pre bezpečnú informačnú spoločnosť – Dialóg, partnerstvo a aktívne pôsobenie [7] sa potvrdzuje, že rôznorodosť, otvorenosť, interoperabilita, využiteľnosť a hospodárska súťaž sú kľúčovými hnacími silami pre bezpečnú informačnú spoločnosť, vyzdvihuje úloha členských štátov a verejnej správy v zlepšovaní informovanosti a v podpore dobrých bezpečnostných predpisov a vyzývajú sa zainteresované strany zo súkromného sektora, aby sa chopili iniciatívy a vypracovali cenovo dostupné systémy osvedčovania bezpečnosti výrobkov, procesov a služieb, ktoré spĺňajú osobitné potreby EÚ, najmä pokiaľ ide o ochranu súkromia.

(16) Uznesenie Rady z 22. marca 2007 [8] o stratégii pre bezpečnú informačnú spoločnosť v Európe vyzýva členské štáty, aby venovali náležitú pozornosť potrebe predchádzať novým a bojovať proti už existujúcim bezpečnostným hrozbám pre elektronické komunikačné siete.

(17) Rámec vypracovaný na úrovni Spoločenstva na vykonávanie posúdení vplyvu na ochranu súkromia a údajov zabezpečí, aby sa ustanovenia tohto odporúčania dodržiavali jednotne vo všetkých členských štátoch. Vypracovanie takéhoto rámca by malo byť založené na existujúcich postupoch a skúsenostiach získaných v členských štátoch, v tretích krajinách a v práci, ktorú vykonáva Európska agentúra pre bezpečnosť sietí a informácií (ENISA – European Network and Information Security Agency) [9].

(18) Komisia zabezpečí vypracovanie usmernení na úrovni Spoločenstva o riadení bezpečnosti informácií pre aplikácie RFID, pričom bude vychádzať z existujúcich postupov a skúseností získaných v členských štátoch a tretích krajinách. Členské štáty by mali prispieť k uvedenému procesu a podporiť účasť súkromných subjektov a verejných orgánov.

(19) Posúdenie vplyvov na ochranu súkromia a údajov vykonané prevádzkovateľom pred realizáciou aplikácie RFID poskytne informácie, ktoré sú potrebné na prijatie primeraných ochranných opatrení. Takéto opatrenia sa budú musieť monitorovať a skúmať počas celej životnosti aplikácie RFID.

(20) V maloobchodnom sektore by posúdenie vplyvov výrobkov obsahujúcich štítky, ktoré sa predávajú spotrebiteľom, na ochranu súkromia a údajov malo poskytnúť potrebné informácie umožňujúce určiť, či existuje pravdepodobná hrozba pre súkromie alebo ochranu osobných údajov.

[1] KOM(2007) 96 v konečnom znení.
[2] Ú. v. ES L 281, 23.11.1995, s. 31.
[3] Ú. v. ES L 201, 31.7.2002, s. 37.
[4] Ú. v. ES L 91, 7.4.1999, s. 10.
[5] Ú. v. EÚ C 101, 23.4.2008, s. 1.
[6] KOM(2007) 228 v konečnom znení.
[7] KOM(2006) 251 v konečnom znení.
[8] Ú. v. EÚ C 68, 24.3.2007, s. 1.
[9] Článok 2 ods. 1 nariadenia Európskeho parlamentu a Rady (ES) č. 460/2004 (Ú. v. EÚ L 77, 13.3.2004, s. 1).

(21) Používanie medzinárodných noriem, napríklad noriem, ktoré vypracovala Medzinárodná organizácia pre normalizáciu (ISO – International Organisation for Standardisation), kódexov správania a najlepších postupov, ktoré sú v súlade s regulačným rámcom EÚ, môže pomôcť pri riadení opatrení v oblasti bezpečnosti informácií a súkromia počas celého obchodného procesu využívajúceho technológiu RFID.

(22) Aplikácie RFID s dosahom na širokú verejnosť, napríklad elektronické cestovné lístky vo verejnej doprave, si vyžadujú primerané ochranné opatrenia. Aplikácie RFID, ktoré majú vplyv na jednotlivcov v dôsledku spracovania napríklad biometrických identifikačných údajov alebo údajov týkajúcich sa zdravotného stavu sú osobitne dôležité, pokiaľ ide o bezpečnosť informácií a súkromie, a preto si vyžadujú osobitnú pozornosť.

(23) Spoločnosť ako celok musí byť informovaná o povinnostiach a právach, ktoré sa uplatňujú v súvislosti s používaním aplikácií RFID. Strany, ktoré zavádzajú túto technológiu, sú preto zodpovedné za poskytnutie informácií o používaní týchto aplikácií verejnosti.

(24) Zvyšovanie informovanosti medzi verejnosťou a malými a strednými podnikmi (MSP) o vlastnostiach a schopnostiach RFID pomôže tomu, aby táto technológia mohla splniť svoj hospodársky prísľub, pričom súčasne zmierni riziko, že sa RFID bude používať na úkor verejného záujmu, čím sa posilní jej prijateľnosť.

(25) Komisia prispeje k vykonávaniu tohto odporúčania priamo a nepriamo podporou dialógu a spolupráce medzi zainteresovanými stranami, najmä prostredníctvom rámcového programu pre konkurencieschopnosť a inovácie (CIP – Competitiveness and Innovation framework Programme) ustanoveného rozhodnutím Európskeho parlamentu a Rady č. 1639/2006/ES [1] a siedmeho rámcového programu v oblasti výskumu (7. RP) ustanoveného rozhodnutím Európskeho parlamentu a Rady č. 1982/2006/ES [2].

(26) Výskum a vývoj nízkonákladových technológií na zvýšenie ochrany súkromia a technológií na zaručenie bezpečnosti informácií je nevyhnutný na úrovni Spoločenstva, aby sa podporilo širšie zavedenie týchto technológií za prijateľných podmienok.

(27) Toto odporúčanie rešpektuje základné práva a dodržiava zásady uznané najmä v Charte základných práv Európskej únie. Cieľom tohto odporúčania je predovšetkým zabezpečiť najmä úplné rešpektovanie súkromného a rodinného života a ochranu osobných údajov,

TÝMTO ODPORÚČA:

Rozsah pôsobnosti

1. Toto odporúčanie poskytuje členským štátom usmernenie k navrhovaniu a prevádzke aplikácií RFID zákonným, etickým a spoločensky a politicky prijateľným spôsobom, tak aby sa zároveň rešpektovalo právo na súkromie a zabezpečila ochrana osobných údajov.

2. Toto odporúčanie poskytuje usmernenie k opatreniam, ktoré sa majú prijať pri zavádzaní aplikácií RFID, aby sa podľa možnosti zabezpečilo dodržiavanie vnútroštátnych právnych predpisov, ktorými sa vykonávajú smernice 95/46/ES, 1999/5/ES a 2002/58/ES, keď sa takéto aplikácie zavedú.

Vymedzenie pojmov

3. Na účely tohto odporúčania by sa mali uplatňovať vymedzenia pojmov uvedené v smernici 95/46/ES. Mali by sa uplatňovať aj tieto vymedzenia pojmov:

a) „rádiofrekvenčná identifikácia“ (RFID) znamená používanie elektromagnetických radiačných vĺn alebo väzby reaktívneho poľa v rádiofrekvenčnej časti spektra na prenesenie na štítok alebo zo štítka prostredníctvom rôznych modulačných a kódovacích systémov s cieľom špecificky prečítať identitu rádiofrekvenčného štítka alebo iné údaje uložené na ňom;

b) „štítok RFID“ alebo „štítok“ znamená buď zariadenie RFID, ktoré dokáže vytvoriť rádiový signál, alebo zariadenie RFID, ktoré znovu spája, spätne rozptyľuje alebo odráža (v závislosti od druhu zariadenia) a moduluje nosný signál získaný z čítačky alebo zapisovačky;

c) „čítačka alebo zapisovačka RFID“ alebo „čítačka“ znamená pevné alebo mobilné zariadenie na zachytávanie a identifikáciu údajov používajúce rádiofrekvenčnú elektromagnetickú vlnu alebo väzbu reaktívneho poľa na stimulovanie a uskutočnenie modulovanej dátovej odpovede zo štítka alebo skupiny štítkov;

d) „aplikácia RFID“ alebo „aplikácia“ znamená aplikáciu, ktorá spracúva údaje prostredníctvom používania štítkov a čítačiek a ktorú podporuje záložný systém a sieťová komunikačná infraštruktúra;

e) „prevádzkovateľ aplikácie RFID“ alebo „prevádzkovateľ“ znamená fyzickú alebo právnickú osobu, verejný orgán, agentúru alebo akýkoľvek iný orgán, ktorý sám alebo spoločne s ostatnými určuje účely a prostriedky prevádzkovania aplikácie vrátane správcov osobných údajov používajúcich aplikáciu RFID;

[1] Ú. v. EÚ L 310, 9.11.2006, s. 15.
[2] Ú. v. EÚ L 412, 30.12.2006, s. 1.

f) „bezpečnosť informácií“ znamená zachovanie dôvernosti, celistvosti a dostupnosti informácií;

g) „monitorovanie“ znamená akúkoľvek činnosť vykonávanú na účely zistenia, sledovania, kopírovania alebo zaznamenania miesta, pohybu, činností alebo stavu jednotlivca.

Posúdenia vplyvu na ochranu súkromia a údajov

4. Členské štáty by mali zabezpečiť, aby priemyselné odvetvie v spolupráci s príslušnými zainteresovanými stranami občianskej spoločnosti vytvorilo rámec na posudzovanie vplyvu na ochranu súkromia a údajov. Tento rámec by sa mal predložiť na schválenie Pracovnej skupine pre ochranu údajov zriadenej podľa článku 29 do 12 mesiacov od uverejnenia tohto odporúčania v *Úradnom vestníku Európskej únie*.

5. Členské štáty by mali zabezpečiť, aby prevádzkovatelia bez ohľadu na svoje ďalšie povinnosti podľa smernice 95/46/ES:

a) posúdili dôsledky realizácie aplikácie pre ochranu osobných údajov a súkromia vrátane posúdenia, či by sa aplikácia mohla používať na monitorovanie jednotlivca. Úroveň podrobnosti posúdenia by mala byť primeraná rizikám pre súkromie, ktoré sú pravdepodobne spojené s aplikáciou;

b) prijali primerané technické a organizačné opatrenia zabezpečujúce ochranu osobných údajov a súkromia;

c) určili osobu alebo skupinu osôb zodpovednú(-ých) za preskúmanie posúdení a nepretržitú primeranosť technických a organizačných opatrení zabezpečujúcich ochranu osobných údajov a súkromia;

d) sprístupnili posúdenie príslušnému orgánu aspoň šesť týždňov pred zavedením aplikácie;

e) po sprístupnení rámca na posudzovanie vplyvov na ochranu súkromia a údajov, ako je ustanovené v bode 4, vykonali uvedené ustanovenia v súlade s rámcom.

Bezpečnosť informácií

6. Členské štáty by mali podporiť Komisiu pri určovaní tých aplikácií, ktoré by mohli ohroziť bezpečnosť informácií s dôsledkami pre širokú verejnosť. V prípade takýchto aplikácií by členské štáty mali zabezpečiť, aby prevádzkovatelia spolu s príslušnými vnútroštátnymi orgánmi a organizáciami občianskej spoločnosti vytvorili nové systémy alebo uplatňovali existujúce systémy, napríklad vydávanie osvedčení alebo samohodnotenie prevádzkovateľa, s cieľom preukázať, že je zavedená primeraná úroveň bezpečnosti informácií a ochrana súkromia vo vzťahu k posúdeným rizikám.

Informácie o používaní RFID a transparentnosť jeho používania

7. Bez toho, aby boli dotknuté povinnosti správcu údajov v súlade so smernicami 95/46/ES a 2002/58/ES, by členské štáty mali zabezpečiť, aby prevádzkovatelia pre každú zo svojich aplikácií vypracovali a uverejnili stručné, presné a zrozumiteľné informačné zásady. Tieto zásady by mali obsahovať aspoň:

a) totožnosť a adresu prevádzkovateľov;

b) účel aplikácie;

c) ktoré údaje má aplikácia spracúvať, najmä ak sa budú spracúvať osobné údaje, a či sa bude monitorovať miesto štítkov;

d) zhrnutie posúdenia vplyvu na ochranu súkromia a údajov;

e) pravdepodobné riziká pre súkromie, ak existujú, týkajúce sa používania štítkov v aplikácii, a opatrenia, ktoré môžu prijať jednotlivci na zmiernenie týchto rizík.

8. Členské štáty by mali zabezpečiť, aby prevádzkovatelia prijali opatrenia na informovanie jednotlivcov o prítomnosti čítačiek na základe spoločnej európskej značky vytvorenej európskymi organizáciami pre normalizáciu s podporou príslušných zainteresovaných strán. Táto značka by mala obsahovať totožnosť prevádzkovateľa a kontaktné miesto, na ktorom môžu jednotlivci získať informácie o aplikácii.

Aplikácie RFID používané v maloobchodnom sektore

9. Na základe spoločnej európskej značky vytvorenej európskymi organizáciami pre normalizáciu s podporou príslušných zainteresovaných strán by prevádzkovatelia mali informovať jednotlivcov o prítomnosti štítkov, ktoré sú umiestnené na výrobkoch alebo sú zakomponované do výrobkov.

10. Pri posudzovaní vplyvov na ochranu súkromia a údajov, ako je uvedené v bodoch 4 a 5, by prevádzkovateľ aplikácie mal osobitne určiť, či štítky umiestnené na výrobkoch alebo zakomponované do výrobkov, ktoré sa predávajú spotrebiteľom prostredníctvom maloobchodníkov, ktorí nie sú prevádzkovateľmi uvedenej aplikácie, predstavujú pravdepodobnú hrozbu pre súkromie alebo ochranu osobných údajov.

11. Maloobchodníci by mali na mieste predaja deaktivovať alebo odstrániť štítky používané v ich aplikácii, pokiaľ spotrebitelia po tom, ako boli informovaní o zásadách uvedených v bode 7, nedajú svoj súhlas so zachovaním funkčnosti štítkov. Deaktivácia štítkov by sa mala chápať ako akýkoľvek proces, ktorý zastaví interakcie štítka s jeho prostredím, ktoré si nevyžadujú aktívne zapojenie spotrebiteľa. Maloobchodník by mal deaktivovať alebo odstrániť štítky pre spotrebiteľa okamžite a bezplatne. Spotrebitelia by mali byť schopní overiť, či skutočne došlo k deaktivácii alebo odstráneniu.

12. Bod 11 by sa nemal uplatňovať, ak sa pri posúdení vplyvu na ochranu súkromia a údajov dospelo k záveru, že štítky, ktoré sa používajú v maloobchodnej aplikácii a ktoré zostanú funkčné po mieste predaja, nepredstavujú pravdepodobnú hrozbu pre súkromie alebo ochranu osobných údajov. Maloobchodníci by však mali bezplatne sprístupniť jednoduché prostriedky na okamžitú alebo neskoršiu deaktiváciu alebo odstránenie týchto štítkov.

13. Deaktivácia alebo odstránenie štítkov by nemalo znamenať žiadne zníženie alebo skončenie zákonných povinností maloobchodníka alebo výrobcu voči spotrebiteľovi.

14. Body 11 a 12 by sa mali vzťahovať iba na maloobchodníkov, ktorí sú prevádzkovateľmi.

Opatrenia na zvýšenie informovanosti

15. Členské štáty by v spolupráci s priemyselným odvetvím, Komisiou a ďalšími zainteresovanými stranami mali prijať primerané opatrenia na informovanie verejných orgánov a spoločností, najmä MSP, a na zvýšenie ich informovanosti o potenciálnych prínosoch a rizikách spojených s používaním technológie RFID. Osobitná pozornosť by sa mala venovať aspektom bezpečnosti informácií a súkromia.

16. Členské štáty by v spolupráci s priemyselným odvetvím, združeniami občianskej spoločnosti, Komisiou a ďalšími zainteresovanými stranami mali určiť a poskytnúť príklady správnych postupov pri realizácii aplikácií RFID s cieľom informovať širokú verejnosť a zvyšovať jej informovanosť. Mali by prijať aj primerané opatrenia, napríklad rozsiahle pilotné projekty, na zvýšenie informovanosti verejnosti o technológii RFID, jej prínosoch, rizikách a dôsledkoch používania, ktoré by boli podmienkou na širšie zavedenie tejto technológie.

Výskum a vývoj

17. Členské štáty by mali spolupracovať s priemyselným odvetvím, príslušnými zainteresovanými stranami občianskej spoločnosti a Komisiou s cieľom stimulovať a podporiť zavedenie zásady „bezpečnosti a ochrany súkromia od návrhu“ už v počiatočnom štádiu vývoja aplikácií RFID.

Následný postup

18. Členské štáty by mali prijať všetky potrebné opatrenia, aby upozornili všetky zainteresované strany, ktoré sú zapojené do návrhu a prevádzky aplikácií RFID v rámci Spoločenstva, na toto odporúčanie.

19. Členské štáty by mali najneskôr do 24 mesiacov od uverejnenia tohto odporúčania v *Úradnom vestníku Európskej únie* informovať Komisiu o opatrení prijatom ako reakcia na toto odporúčanie.

20. Do troch rokov od uverejnenia tohto odporúčania v *Úradnom vestníku Európskej únie* Komisia predloží správu o vykonávaní tohto odporúčania, jeho účinnosti a vplyve na prevádzkovateľov a spotrebiteľov, najmä pokiaľ ide o opatrenia odporúčané v bodoch 9 až 14.

Adresáti

21. Toto odporúčanie je určené členským štátom.

V Bruseli 12. mája 2009

Za Komisiu

Viviane REDING

členka Komisie