PRIPOROČILA

KOMISIJA

PRIPOROČILO KOMISIJE

z dne 12. maja 2009

o izvajanju načel varstva zasebnosti in varstva podatkov v aplikacijah, podprtih z radiofrekvenčno identifikacijo

(notificirano pod dokumentarno številko C(2009) 3200)

(2009/387/ES)

KOMISIJA EVROPSKIH SKUPNOSTI –

ob upoštevanju Pogodbe o ustanovitvi Evropske skupnosti in zlasti člena 211 Pogodbe,

po posvetovanju z evropskim nadzornikom za varstvo podatkov,

ob upoštevanju naslednjega:

(1) Radiofrekvenčna identifikacija (RFID) označuje nov razvoj v informacijski družbi, kjer bodo predmeti, opremljeni z mikroelektronskimi komponentami, ki lahko avtomatično obdelujejo podatke, vedno bolj del vsakodnevnega življenja.

(2) RFID je vse bolj razširjen in zato del posameznikovega življenja na različnih področjih, kot so logistika ([1]), zdravstveno varstvo, javni prevoz, trgovina na drobno (predvsem za boljšo varnost izdelkov in hitrejši odpoklic izdelkov), razvedrilo, delo, upravljanje cestninjenja in prtljage ter potovalni dokumenti.

(3) Tehnologija RFID lahko postane nova gonilna sila rasti in delovnih mest ter tako bistveno prispeva k lizbonski strategiji, saj veliko obeta v gospodarskem smislu, kjer lahko zagotovi nove poslovne priložnosti, zniža stroške in poveča učinkovitost, predvsem pri odpravljanju ponarejanja in ravnanju z e-odpadki in nevarnimi snovmi ter recikliranju izdelkov po koncu njihove življenjske dobe.

(4) Tehnologija RFID omogoča obdelavo podatkov, vključno z osebnimi podatki, na kratke razdalje, brez fizičnega stika ali vidne interakcije med čitalnikom ali pisalnikom in oznako, tako da je mogoča taka interakcija, ne da bi se je posameznik zavedal.

(5) Aplikacije RFID lahko obdelujejo podatke, ki se nanašajo na določeno ali določljivo fizično osebo, kar pomeni, da se lahko fizična oseba identificira neposredno ali posredno. Lahko obdelujejo osebne podatke, shranjene na oznaki, kot so ime, datum rojstva in naslov ali biometrični podatki osebe, ali pa podatke, ki določeno številko postavke RFID povezujejo z osebnimi podatki, shranjenimi drugod v sistemu. Ta tehnologija se lahko uporablja tudi za spremljanje posameznikov, ki imajo pri sebi enega ali več predmetov, ki vsebujejo številko postavke RFID.

(6) Ker je tehnologija RFID lahko povsod uporabljena in je pravzaprav nevidna, je treba pri njeni uvedbi nameniti posebno pozornost vprašanjem varstva zasebnosti in podatkov. Zato je treba v aplikacije RFID pred njihovo širšo uporabo vgraditi varovalne lastnosti za varstvo zasebnosti in informacij(načelo „varstva in zasebnosti pri snovanju sistemov“).

(7) RFID bo lahko zagotovil številne gospodarske in družbene koristi le, če se bodo izvajali učinkoviti ukrepi za zagotavljanje varstva osebnih podatkov, zasebnosti in s tem povezanih etičnih načel, ključnih v razpravi o javni sprejetosti RFID.

(8) Države članice in zainteresirane strani bi si morale predvsem v tej začetni fazi uvajanja RFID prizadevati tudi za to, da bodo zagotovile, da so aplikacije RFID pod nadzorom ter da se spoštujejo pravice in svoboščine posameznikov.

([1]) COM(2007) 607 konč.

(9) Komisija je v sporočilu z dne 15. marca 2007 „Radiofrekvenčna identifikacija (RFID) v Evropi: naslednji koraki v okviru politike“ [1] napovedala, da naj bi v enem ali več priporočilih pripravila pojasnila in smernice o vidikih varstva podatkov in zasebnosti pri aplikacijah RFID.

(10) Pravice in obveznosti v zvezi z varstvom osebnih podatkov in prostim pretokom takih podatkov, kot jih določata Direktiva Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov [2] ter Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) [3], veljajo v celoti za aplikacije RFID, s katerimi se obdelujejo osebni podatki.

(11) Pri razvoju aplikacij RFID se uporabljajo načela, določena v Direktivi 1999/5/ES Evropskega parlamenta in Sveta z dne 9. marca 1999 o radijski opremi in telekomunikacijski terminalski opremi ter medsebojnem priznavanju skladnosti te opreme [4].

(12) Evropski nadzornik za varstvo podatkov [5] v svojem mnenju zagotovi smernice za obravnavanje izdelkov, ki vsebujejo oznake in so namenjeni posameznikom, ter poziva k oceni učinka na varstvo zasebnosti in varstvo podatkov, da bi pri sistemih RFID opredelili in razvili „najboljše razpoložljive tehnologije“ za zagotavljanje zasebnosti in varstva podatkov.

(13) Upravljavci aplikacij RFID bi morali sprejeti vse ustrezne ukrepe, s katerimi bi zagotovili, da se s sredstvi, ki bi jih lahko uporabil upravljavec aplikacije RFID ali katera koli druga oseba podatki ne nanašajo na določene ali določljive fizične osebe, razen če so taki podatki obdelani v skladu z veljavnimi načeli in pravnimi predpisi o varstvu podatkov.

(14) V sporočilu Komisije z dne 2. maja 2007 z naslovom Spodbujanje varstva podatkov za boljše varovanje zasebnosti (PET) [6] so določeni jasni ukrepi, s katerimi bi dosegli čim manjšo obdelavo osebnih podatkov in uporabo anonimnih ali psevdonimnih podatkov, in sicer s spodbujanjem razvoja tehnologij za izboljšanje varstva zasebnosti in njihove uporabe za upravljavce podatkov in posameznike.

(15) Komisija v sporočilu z dne 31. maja 2006 z naslovom Strategija za varno informacijsko družbo – dialog, partnerstvo ter povečanje vpliva in moči [7] ugotavlja, da so raznolikost, odprtost, interoperabilnost, uporabnost in konkurenčnost ključni dejavniki varne informacijske družbe, poudarja vlogo držav članic in javnih uprav pri izboljševanju ozaveščenosti in pospeševanju dobrih varnostnih praks ter poziva zainteresirane strani v zasebnem sektorju, naj sprejmejo pobude, s katerimi bodo zagotovile cenovno dostopne varnostne sheme za potrjevanje izdelkov, procesov in storitev, ki bodo obravnavale potrebe EU, zlasti glede zasebnosti.

(16) Svet v resoluciji z dne 22. marca 2007 o strategiji za varno informacijsko družbo v Evropi [8] poziva države članice, naj namenijo ustrezno pozornost preprečevanju in boju proti novim in že znanim varnostnim grožnjam za elektronska komunikacijska omrežja.

(17) Okvir, razvit na ravni Skupnosti za izvajanje ocen učinka na varstvo zasebnosti in podatkov, bo zagotovil, da bodo določbe tega priporočila enotno upoštevale vse države članice. Razvoj takega okvira naj bi temeljil na uveljavljenih praksah in izkušnjah, pridobljenih v državah članicah, tretjih državah in z delom, ki ga je opravila Evropska agencija za varnost omrežij in informacij (ENISA) [9].

(18) Komisija bo na ravni Skupnosti zagotovila razvoj smernic za upravljanje varnosti informacij za aplikacije RFID, pri čemer bo upoštevala uveljavljene prakse in izkušnje, ki so jih pridobile države članice in tretje države. Države članice bi morale prispevati k temu procesu ter zasebne subjekte in javne organe spodbujati k sodelovanju.

(19) Ocena učinkov na varstvo zasebnosti in podatkov, ki jo pred izvajanjem aplikacije RFID opravi upravljavec, bo vsebovala informacije, potrebne za ustrezne varnostne ukrepe. Take ukrepe bo treba spremljati in pregledovati celotno življenjsko dobo aplikacije RFID.

(20) V trgovini na drobno naj bi ocena učinkov na varstvo zasebnosti in podatkov pri izdelkih, ki vsebujejo oznake in ki se prodajajo potrošnikom, zagotovila potrebne informacije, s katerimi bi bilo mogoče ugotoviti, ali je ogrožanje varstva zasebnosti ali podatkov verjetna.

[1] COM(2007) 96 konč.
[2] UL L 281, 23.11.1995, str. 31.
[3] UL L 201, 31.7.2002, str. 37.
[4] UL L 91, 7.4.1999, str. 10.
[5] UL C 101, 23.4.2008, str. 1.
[6] COM (2007) 228 konč.
[7] COM(2006) 251 konč.
[8] UL C 68, 24.3.2007, str. 1.
[9] Člen 2(1) Uredbe (ES) št. 460/2004 Evropskega parlamenta in Sveta.

(21) Uporaba mednarodnih standardov, kot jih je npr. razvila Mednarodna organizacija za standardizacijo (ISO), kodeksov ravnanja in najboljših praks, ki so v skladu s pravnim okvirom EU, lahko pomaga pri upravljanju ukrepov za zagotovitev varnosti informacij in varstva zasebnosti v celotnem poslovnem procesu, ki je podprt z RFID.

(22) Aplikacije RFID, ki vplivajo na širšo javnost, npr. elektronske vozovnice v javnem prevozu, bi bilo treba ustrezno zaščititi z varnostnimi ukrepi. Aplikacije RFID, ki vplivajo na posameznike, ker npr. obdelujejo podatke za biometrično identifikacijo ali zdravstvene podatke, so glede varnosti informacij in zasebnosti še posebej kritične in jim je zato treba nameniti posebno pozornost.

(23) Družba kot celota se mora zavedati obveznosti in pravic, ki veljajo za uporabo aplikacij RFID. Tisti, ki uvajajo to tehnologijo, so zato odgovorni, da posameznikom zagotovijo informacije o uporabi teh aplikacij.

(24) Povečevanje ozaveščenosti v javnosti ter v malih in srednje velikih podjetjih (MSP) o lastnostih in zmogljivostih RFID bo pripomoglo k temu, da bo ta tehnologija izpolnila gospodarska pričakovanja ter hkrati ublažilo tveganje, da bi jo uporabili v škodo javnemu interesu, kar bo povečalo njeno sprejemljivost.

(25) Komisija bo k izvajanju tega priporočila prispevala neposredno in posredno, tako da bo spodbujala dialog in sodelovanje med zainteresiranimi stranmi, zlasti z okvirnim programom za konkurenčnost in inovativnost (CIP), ustanovljenim s sklepom Evropskega parlamenta in Sveta št. 1639/2006/ES ([1]), in s sedmim okvirnim programom za raziskave (FP7), ustanovljenim s sklepom Evropskega parlamenta in Sveta št. 1982/2006/ES ([2]).

(26) Raziskave in razvoj na ravni Skupnosti za stroškovno ugodne tehnologije za povečevanje varstva zasebnosti in tehnologije za varnost informacij so ključni za spodbujanje širšega uvajanja teh tehnologij pod sprejemljivimi pogoji.

(27) V tem priporočilu so upoštevane temeljne pravice in načela, ki jih zlasti priznava Listina Evropske unije o temeljnih pravicah. Njegov namen je zagotoviti celovito spoštovanje zasebnega in družinskega življenja ter varstva osebnih podatkov –

([1]) UL L 310, 9.11.2006, str. 15.
([2]) UL L 412, 30.12.2006, str. 1.

PRIPOROČA:

Področje uporabe

1. To priporočilo vsebuje smernice za države članice o zasnovi in delovanju aplikacij RFID na zakonit, etičen ter družbeno in politično sprejemljiv način ter ob spoštovanju pravice do zasebnosti in zagotavljanju varstva osebnih podatkov.

2. To priporočilo vsebuje smernice za ukrepe, ki jih je treba sprejeti pri uvedbi aplikacij RFID, da se pri uvedbi, kjer je primerno, zagotovi spoštovanje nacionalne zakonodaje, s katero so bile prenesene direktive 95/46/ES, 1999/5/ES in 2002/58/ES.

Opredelitev pojmov

3. Za namene tega priporočila se uporabljajo opredelitve pojmov iz direktive 95/46/ES. Uporabljajo se tudi naslednje opredelitve pojmov:

(a) „radiofrekvenčna identifikacija“ (RFID) pomeni uporabo elektromagnetnih valov ali povezovanje reaktivnih polj v radiofrekvenčnem delu za komunikacijo iz oznake ali vanjo prek različnih tehnik modulacije ali kodiranja, zgolj za identifikacijo radiofrekvenčne oznake ali na njej shranjenih podatkov;

(b) „oznaka RFID“ ali „oznaka“ pomeni napravo RFID, ki lahko proizvede radijski signal, ali napravo RFID, ki razveže, razprši nazaj ali odbije (odvisno od tipa naprave) in modulira nosilni signal, prejet od čitalnika ali pisalnika;

(c) „čitalnik ali pisalnik RFID“ ali „čitalnik“ pomeni fiksno ali mobilno napravo za zajem in identifikacijo podatkov, ki uporablja radiofrekvenčni elektromagnetni val ali povezovanje reaktivnih polj, da spodbudi in povzroči odziv oznake ali skupine oznake v obliki moduliranih podatkov;

(d) „aplikacija RFID“ ali „aplikacija“ pomeni aplikacijo, ki obdeluje podatke tako, da uporablja oznake in čitalnike, pri tem pa je podprta z zalednim sistemom in mrežno komunikacijsko infrastrukturo;

(e) „upravljavec aplikacije RFID“ ali „upravljavec“ pomeni fizično ali pravno osebo, javni organ, agencijo ali kateri koli drug organ, ki sam ali skupaj z drugimi določa namene in načine delovanja aplikacije, vključno z upravljavci osebnih podatkov, ki uporabljajo aplikacijo RFID;

(f) „varnost informacij“ pomeni ohranjanje zaupnosti, celovitosti in razpoložljivosti informacij;

(g) „spremljanje“ pomeni kakršno koli dejavnost, ki se izvaja z namenom odkrivanja, opazovanja, posnemanja ali zapisovanja lokacije, premikanja, dejavnosti ali stanja posameznika.

Ocene učinka na varstvo zasebnosti inpodatkov

4. Države članice zagotovijo, da stroka v sodelovanju z ustreznimi zainteresiranimi stranmi civilne družbe razvije okvir za ocenjevanje učinkov na varstvo zasebnosti in podatkov. Ta okvir se predloži v potrditev delovni skupini za varstvo podatkov iz člena 29 v 12 mesecih po objavi tega priporočila v *Uradnem listu Evropske unije*.

5. Države članice zagotovijo, da upravljavci ne glede na svoje obveznosti v skladu z direktivo št. 95/46/ES:

(a) ocenijo posledice izvajanja aplikacije na varstvo osebnih podatkov in zasebnosti ter preverijo, ali bi aplikacijo lahko uporabljali za nadzorovanje posameznika. Podrobnost ocene mora ustrezati tveganjem za zasebnost, povezanim z aplikacijo;

(b) sprejmejo ustrezne tehnične in organizacijske ukrepe, s katerimi zagotovijo varstvo osebnih podatkov in zasebnosti;

(c) imenujejo osebo ali skupino oseb, odgovorno za pregledovanje ocen in nenehne ustreznosti tehničnih in organizacijskih ukrepov za zagotovitev varstva osebnih podatkov in zasebnosti;

(d) zagotovijo, da je ocena na voljo pristojnemu organu vsaj šest tednov pred uvedbo aplikacije;

(e) po določitvi okvira za ocenjevanje učinka na varstvo zasebnosti in podatkov iz točke 4 izvajajo zgornje določbe v skladu z njim.

Varnost informacij

6. Države članice podpirajo Komisijo pri opredeljevanju tistih aplikacij, ki bi lahko ogrožale varnost informacij in imele posledice za širšo javnost. Pri takih aplikacijah države članice zagotovijo, da upravljavci, skupaj s pristojnimi nacionalnimi organi in organizacijami civilne družbe, razvijejo nove sheme ali uporabijo že uveljavljene sheme, kot je certificiranje ali samoocenjevanje upravljavca, s čimer dokažejo, da je glede na ocenjena tveganja vzpostavljena ustrezna raven varnosti informacij in varstva zasebnosti.

Informacije o uporabi in preglednost uporabe RFID

7. Ne glede na obveznosti upravljavcev podatkov v skladu z direktivo št. 95/46/ES in direktivo št. 2002/58/ES države članice zagotovijo, da upravljavci za vsako od aplikacij razvijejo in objavijo strnjene, natančne in razumljive informacije. Te informacije vsebujejo najmanj:

(a) ime in naslov upravljavcev;

(b) namen aplikacije;

(c) katere podatke bo obdelovala aplikacija, zlasti če bo obdelovala osebne podatke, in ali bo mesto oznak nadzirano;

(d) povzetek ocene učinka na varstvo zasebnosti in podatkov;

(e) morebitna tveganja za zasebnost, ki so povezana z uporabo oznak v aplikaciji, in ukrepe, ki jih lahko posamezniki sprejmejo za ublažitev teh tveganj.

8. Države članice zagotovijo, da upravljavci sprejmejo ukrepe za obveščanje posameznikov o uporabi čitalnikov, in sicer s skupnim evropskim znakom, ki ga razvijejo evropske organizacije za standardizacijo ob podpori vključenih zainteresiranih strani. Znak mora vsebovati identiteto upravljavca in kontaktno točko, kjer lahko posamezniki dobijo informacije o aplikaciji.

Aplikacije RFID, ki se uporabljajo v trgovini na drobno

9. Upravljavci s skupnim evropskim znakom, ki ga razvijejo evropske organizacije za standardizacijo ob podpori vključenih zainteresiranih strani, obvestijo posameznike o uporabi oznak, nameščenih ali vgrajenih v izdelke.

10. Pri pripravljanju ocene učinka na varstvo zasebnosti in podatkov iz točk 4 in 5 upravljavec aplikacije posebej opredeli, ali oznake, nameščene ali vgrajene v izdelke, ki se potrošnikom prodajajo pri trgovcih na drobno, ki niso upravljavci navedene aplikacije, pomenijo tveganje za zasebnost ali varstvo osebnih podatkov.

11. Trgovci na drobno na prodajnem mestu deaktivirajo ali odstranijo oznake, uporabljene v njihovi aplikaciji, razen če se potrošniki po prejetju informacij iz točke 7 strinjajo, da bodo delujoče oznake ohranili. Deaktiviranje oznak pomeni kateri koli proces, ki ustavi interakcijo oznake z njenim okoljem, za katero ni potrebna dejavna vloga potrošnika. Deaktiviranje ali odstranitev oznake opravi trgovec na drobno za potrošnika nemudoma in brezplačno. Potrošnikom mora biti omogočeno, da preverijo, ali je bilo deaktiviranje oziroma odstranitev učinkovita.

12. Točka 11 se ne uporablja, če je v oceni učinka na varstvo zasebnosti in varstvo podatkov ugotovljeno, da oznake, uporabljene v aplikaciji v trgovini na drobno, ki delujejo tudi zunaj prodajnega mesta, ne pomenijo morebitnega tveganja za zasebnost ali varstvo osebnih podatkov. Kljub temu morajo trgovci na drobno zagotoviti brezplačen in preprost način za takojšnjo ali poznejšo deaktiviranje ali odstranitev teh oznak.

13. Pravne obveznosti trgovca na drobno ali proizvajalca do potrošnika se z deaktiviranjem ali odstranitvijo oznak ne zmanjšajo ali prenehajo veljati.

14. Točki 11 in 12 se uporabljata le za trgovce na drobno, ki so upravljavci.

Ukrepi za povečevanje ozaveščenosti

15. Države članice v sodelovanju s stroko, Komisijo in drugimi zainteresiranimi stranmi sprejmejo ustrezne ukrepe za obveščanje in povečevanje ozaveščenosti javnih organov in družb, zlasti malih in srednje velikih podjetij, o morebitnih prednostih in tveganjih, povezanih z uporabo tehnologije RFID. Posebno pozornost morajo nameniti vidikom varnosti informacij in varstva zasebnosti.

16. Države članice v sodelovanju s stroko, organizacijami civilne družbe, Komisijo in drugimi ustreznimi zainteresiranimi stranmi ugotovijo in zagotovijo primere dobre prakse pri uvajanju aplikacij RFID, da bi obvestile širšo javnost in povečale njeno ozaveščenost. Izvajati morajo tudi ustrezne ukrepe, npr. obsežne pilotne projekte, s katerimi povečujejo ozaveščenost javnosti o tehnologiji RFID, njenih prednostih, tveganjih in posledicah uporabe, kar je pogoj za širšo uvedbo te tehnologije.

Raziskave in razvoj

17. Države članice sodelujejo s stroko, ustreznimi zainteresiranimi stranmi civilne družbe in Komisijo, da bi spodbudile in podprle uvedbo načela „varnosti in varstva zasebnosti pri snovanju sistemov“ že na začetku razvoja aplikacij RFID.

Spremljanje

18. Države članice sprejmejo vse ukrepe, potrebne za to, da se to priporočilo predstavi vsem zainteresiranim stranem, ki sodelujejo pri snovanju in delovanju aplikacij RFID v Skupnosti.

19. Države članice najpozneje 24 mesecev po objavi tega priporočila v *Uradnem listu Evropske unije* obvestijo Komisijo o ukrepih, s katerimi so se odzvale na to sporočilo.

20. V treh letih po objavi tega priporočila v *Uradnem listu Evropske unije* bo Komisija predložila poročilo o izvajanju tega priporočila, njegovi učinkovitosti in učinku na upravljavce in potrošnike, zlasti glede ukrepov iz točk 9 do 14.

Naslovniki

21. To priporočilo je naslovljeno na države članice.

V Bruslju, 12. maja 2009

Za Komisijo
Viviane REDING
Članica Komisije