

DOPORUČENÍ

KOMISE

DOPORUČENÍ KOMISE

ze dne 12. května 2009

o zavedení zásad ochrany soukromí a údajů v aplikacích podporovaných identifikací na základě rádiové frekvence

(oznámeno pod číslem K(2009) 3200)

(2009/387/ES)

KOMISE EVROPSKÝCH SPOLEČENSTVÍ,

s ohledem na Smlouvu o založení Evropského společenství, a zejména na článek 211 této smlouvy,

po konzultaci s evropským inspektorem ochrany údajů,

vzhledem k těmto důvodům:

- (1) Identifikace na základě rádiové frekvence (RFID) předznamenává nový vývoj v informační společnosti, kdy se předměty vybavené mikroelektronikou, která může automaticky zpracovávat údaje, budou stále více stávat nedílnou součástí každodenního života.
- (2) RFID je postupně stále běžnější, stává se tudíž součástí života jednotlivců v různých oblastech, jako je logistika⁽¹⁾, zdravotnictví, veřejná doprava, maloobchod, zejména v zájmu větší bezpečnosti výrobků a rychlejšího stažení výrobků z trhu, zábava, práce, správa mýtného, odbavování zavazadel a cestovní doklady.
- (3) Technologie RFID se může stát novou hnací silou růstu a tvorby pracovních příležitostí, a tak významně přispět k Lisabonské strategii, jelikož je velmi slibná z hospodářského hlediska, kde může zajistit nové obchodní příležitosti, snížení nákladů a vyšší účinnost, zejména v boji proti padělání a při nakládání s elektronickým odpadem, nebezpečným materiálem a při recyklaci výrobků na konci jejich životnosti.

- (4) Technologie RFID umožňuje zpracovávat údaje, včetně osobních údajů, na krátké vzdálenosti bez fyzického kontaktu či viditelné interakce mezi čtecím nebo zapisovacím zařízením a etiketou, takže k této interakci může dojít, aniž by si toho byl dotyčný jednotlivec vědom.
- (5) Aplikace RFID mohou zpracovávat údaje týkající se fyzické osoby, jejíž totožnost je zjištěna nebo se má zjistit, a to přímo či nepřímo. Mohou zpracovávat osobní údaje uložené na etiketě, například jméno dotyčné osoby, její datum narození nebo adresu či biometrické údaje nebo údaje spojující určité číslo výrobku RFID s osobními údaji uloženými jinde v systému. Tuto technologii lze využít ke sledování jednotlivců, pokud tito vlastní jeden či více výrobků, které obsahují číslo výrobku RFID.
- (6) Vzhledem k potenciálu této technologie být všudypřítomná a prakticky neviditelná je při zavádění RFID nutno věnovat zvláštní pozornost otázkám ochrany soukromí a údajů. Do aplikací by proto měly být před jejich rozšířením používáním zabudovány bezpečnostní prvky s ohledem na soukromí a informace (zásada „konstrukčního návrhu nenarušujícího bezpečnost a soukromí“).
- (7) RFID může přinést četné hospodářské a společenské výhody pouze tehdy, budou-li zavedena účinná opatření k zajištění ochrany osobních údajů, soukromí a souvisejících etických zásad, jež jsou ústředním bodem diskuse o přijetí RFID ze strany veřejnosti.
- (8) Členské státy a zúčastněné osoby by měly zejména v této počáteční fázi zavádění RFID vynaložit další úsilí s cílem zajistit, aby aplikace RFID byly sledovány a aby byla respektována práva a svobody jednotlivců.

⁽¹⁾ KOM(2007) 607 v konečném znění.

- (9) Sdělení Komise ze dne 15. března 2007 „Identifikace na základě rádiové frekvence (RFID) v Evropě: kroky k rámci politiky“⁽¹⁾ oznámilo, že budou poskytnuta objasnění a pokyny k aspektům ochrany údajů a soukromí v souvislosti s aplikacemi RFID prostřednictvím jednoho či více doporučení Komise.
- (10) Práva a povinnosti týkající se ochrany osobních údajů a volného pohybu těchto údajů, jak jsou stanoveny ve směrnici Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů⁽²⁾ a směrnici Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích)⁽³⁾, jsou plně použitelné na aplikace RFID, které zpracovávají osobní údaje.
- (11) Při vývoji aplikací RFID je nutno uplatňovat zásady stanovené ve směrnici Evropského parlamentu a Rady 1999/5/ES ze dne 9. března 1999 o rádiových zařízeních a telekomunikačních koncových zařízeních a vzájemném uznávání jejich shody⁽⁴⁾.
- (12) Stanovisko evropského inspektora ochrany údajů⁽⁵⁾ poskytuje vodítko pro nakládání s výrobky obsahujícími etikety, které jsou poskytovány jednotlivcům a vyžaduje posouzení dopadů na soukromí a bezpečnost k určení a vypracování „nejlepších dostupných technologií“ v zájmu zajištění soukromí a bezpečnosti systémů RFID.
- (13) Provozovatelé aplikací RFID by měli přijmout veškerá přiměřená opatření s cílem zajistit, aby se údaje nevztahovaly na fyzickou osobu, jejíž totožnost je zjištěna nebo se má zjistit, prostřednictvím jakýchkoli prostředků, jež budou pravděpodobně použity provozovatelem aplikace RFID či jinou osobou, nejsou-li tyto údaje zpracovávány v souladu s platnými zásadami a právními předpisy o ochraně údajů.
- (14) Sdělení Komise ze dne 2. května 2007 o „podpoře ochrany osobních údajů prostřednictvím technologií zvyšujících ochranu soukromí (PETs)“⁽⁶⁾ stanoví jasná opatření k dosažení cíle týkajícího se minimalizace zpracování osobních údajů a tam, kde je to možné, využívání anonymních nebo pseudonymních údajů podporou vývoje PETs a jejich využívání správci údajů a jednotlivci.
- (15) Sdělení Komise ze dne 31. května 2006 Strategie pro bezpečnou informační společnost – „Dialog, partnerství a posílení účasti“⁽⁷⁾ uznává, že rozmanitost, otevřenost, interoperabilita, použitelnost a hospodářská soutěž jsou hlavními hnacími silami pro bezpečnou informační společnost, vyzdvihuje úlohu členských států a orgánů veřejné správy při zvyšování informovanosti a prosazování dobrých bezpečnostních postupů a vyzývá zúčastněné strany ze soukromého sektoru, aby přijaly iniciativy s cílem pracovat na cenově dostupných programech osvědčování bezpečnosti pro produkty, procesy a služby, které budou zohledňovat specifické potřeby EU zejména s ohledem na ochranu soukromí.
- (16) Usnesení Rady ze dne 22. března 2007⁽⁸⁾ o strategii pro bezpečnou informační společnost v Evropě členské státy vyzývá, aby věnovaly náležitou pozornost potřebě zamezit novým a stávajícím bezpečnostním hrozbám pro elektronické komunikační sítě.
- (17) Rámec vypracovaný na úrovni Společenství pro posuzování dopadů na soukromí a ochranu údajů zajistí, aby ustanovení tohoto doporučení byla jednotně dodržována ve všech členských státech. Vypracování takového rámce by mělo navazovat na stávající postupy a zkušenosti získané v členských státech, ve třetích zemích a při práci Evropské agentury pro bezpečnost sítí a informací (ENISA)⁽⁹⁾.
- (18) Komise zajistí vypracování pokynů na úrovni Společenství k řízení bezpečnosti informací pro aplikace RFID, které navazují na stávající postupy a zkušenosti získané v členských státech a třetích zemích. Členské státy by měly přispět k tomuto procesu a vybízet soukromé subjekty a orgány veřejné správy k účasti.
- (19) Posouzení dopadů na soukromí a ochranu údajů provedené provozovatelem před zavedením aplikace RFID poskytne informace potřebné pro náležitá ochranná opatření. Tato opatření je nutno sledovat a přezkoumávat po celou dobu používání aplikace RFID.
- (20) V odvětví maloobchodu by mělo posouzení dopadů výrobků obsahujících etikety, které jsou prodávány spotřebitelům, na soukromí a ochranu údajů poskytnout potřebné informace s cílem určit, zda existuje pravděpodobná hrozba pro soukromí nebo ochranu osobních údajů.

(1) KOM(2007) 96 v konečném znění.

(2) Úř. věst. L 281, 23.11.1995, s. 31.

(3) Úř. věst. L 201, 31.7.2002, s. 37.

(4) Úř. věst. L 91, 7.4.1999, s. 10.

(5) Úř. věst. C 101, 23.4.2008, s. 1.

(6) KOM(2007) 228 v konečném znění.

(7) KOM(2006) 251 v konečném znění.

(8) Úř. věst. C 68, 24.3.2007, s. 1.

(9) Čl. 2 odst. 1 nařízení (ES) č. 460/2004 Evropského parlamentu a Rady (Úř. věst. L 77, 13.3.2004, s. 1).

- (21) Řízení bezpečnosti informací a opatření na ochranu soukromí v celém obchodním procesu umožněném RFID může napomoci používání mezinárodních norem, například norem vypracovaných Mezinárodní organizací pro normalizaci (ISO), kodexů chování a osvědčených postupů, jež jsou v souladu s právním rámcem EU.
- (22) Aplikace RFID s důsledky pro širokou veřejnost, například elektronické jízdenky ve veřejné dopravě, vyžadují vhodná ochranná opatření. Aplikace RFID, které se dotýkají jednotlivce například zpracováním biometrických identifikačních údajů nebo údajů souvisejících se zdravím, jsou obzvláště kritické, pokud jde o bezpečnost informací a soukromí, a vyžadují proto zvláštní pozornost.
- (23) Celá společnost musí být informována o povinnostech a právech, jež jsou platné s ohledem na používání aplikací RFID. Strany, které zavádějí tuto technologii, proto odpovídají za informování jednotlivců o používání těchto aplikací.
- (24) Zvyšování informovanosti veřejnosti a malých a středních podniků o charakteristikách a schopnostech RFID pomůže této technologii naplnit hospodářská očekávání a současně zmírnit rizika toho, že bude použita na úkor veřejného zájmu, zvýšit tudíž její přijatelnost.
- (25) Komise přispěje k provádění tohoto doporučení přímo a nepřímou usnadněním dialogu a spolupráce mezi zúčastněnými stranami, zejména prostřednictvím rámcového programu pro konkurenceschopnost a inovace zřízeného rozhodnutím Evropského parlamentu a Rady č. 1639/2006/ES ⁽¹⁾ a sedmého rámcového programu pro výzkum (7. RP) zřízeného rozhodnutím Evropského parlamentu a Rady č. 1982/2006/ES ⁽²⁾.
- (26) Na úrovni Společenství je nezbytný výzkum a vývoj nízkonákladových technologií na podporu ochrany soukromí a technologií pro bezpečnost informací k prosazování širšího přijetí těchto technologií za příjatečných podmínek.
- (27) Toto doporučení dodržuje základní práva a ctí zásady uznávané zejména Listinou základních práv Evropské unie. Cílem tohoto doporučení je zejména zajistit respektování soukromého a rodinného života a ochrany osobních údajů,

DOPORUČUJE:

Oblast působnosti

1. Toto doporučení poskytuje členským státům vodítko při navrhování a provozování aplikací RFID zákonným, etickým a sociálně a politicky přijatelným způsobem při současném dodržování práva na soukromí a zajištění ochrany osobních údajů.
2. Toto doporučení poskytuje pokyny k opatřením, jež je nutno přijmout s ohledem na zavádění aplikací RFID s cílem zajistit, aby při používání těchto aplikací byly popřípadě dodržovány vnitrostátní právní předpisy k provedení směrnic 95/46/ES, 1999/5/ES a 2002/58/ES.

Definice

3. Pro účely tohoto doporučení se použijí definice stanovené ve směrnici 95/46/ES. Použijí se rovněž tyto definice:
 - a) „identifikací na základě rádiové frekvence“ (RFID) se rozumí využívání elektromagnetických vln nebo magnetického pole v části spektra rádiových frekvencí ke komunikaci s etiketou prostřednictvím různých modulárních a kódovacích systémů z účelem jednoznačného přečtení identity etikety nebo jiných údajů, které jsou na ní uloženy;
 - b) „etiketou RFID“ nebo „etiketou“ se rozumí zařízení RFID, které je schopné vytvářet rádiový signál, nebo zařízení RFID, jež opětovně spojuje, zpětně rozptyluje nebo odráží (podle druhu zařízení) a moduluje nosný signál přijatý ze čtecího nebo zapisovacího zařízení;
 - c) „čtecím nebo zapisovacím zařízením RFID“ nebo „čtečkou“ se rozumí pevné nebo přenosné zařízení k zachycování a identifikaci údajů pomocí vysokofrekvenčních elektromagnetických vln nebo magnetického pole ke stimulaci a vyvolání odezvy modulovaných dat z etikety nebo skupiny etiket;
 - d) „aplikací RFID“ nebo „aplikací“ se rozumí aplikace, která zpracovává údaje pomocí etiket a čteček a která je podporována záložním systémem a sítovou komunikační infrastrukturou;
 - e) „provozovatelem aplikace RFID“ nebo „provozovatelem“ se rozumí fyzická nebo právnická osoba, orgán veřejné správy, úřad nebo jiný subjekt, který sám či společně s ostatními stanoví účel a způsoby provozování aplikace, včetně správců osobních údajů používajících aplikaci RFID;

⁽¹⁾ Úř. věst. L 310, 9.11.2006, s. 15.

⁽²⁾ Úř. věst. L 412, 30.12.2006, s. 1.

- f) „bezpečností informací“ se rozumí zachování důvěrnosti, integrity a dostupnosti informací;
- g) „sledováním“ se rozumí jakákoliv činnost vykonávaná za účelem zjištění, pozorování, reprodukování nebo zaznamenání údajů o místě, na němž se jednotlivec nachází, jeho pohybu, činnosti nebo stavu.

Posouzení dopadů na soukromí a ochranu údajů

4. Členské státy by měly zajistit, aby odvětví ve spolupráci s příslušnými zúčastněnými stranami z občanské společnosti vypracovalo rámec pro posuzování dopadů na soukromí a ochranu údajů. Tento rámec by měl být předložen ke schválení pracovní skupině pro ochranu údajů zřízené podle článku 29 do dvanácti měsíců ode dne vyhlášení tohoto doporučení v *Úředním věstníku Evropské unie*.
5. Členské státy by měly zajistit, aby provozovatelé bez ohledu na své povinnosti podle směrnice 95/46/ES:
- a) prováděli posuzování důsledků zavedení aplikace pro ochranu osobních údajů a soukromí, včetně toho, zda by bylo možno aplikaci využít ke sledování jednotlivce. Úroveň podrobnosti tohoto posouzení by měla odpovídat hrozbě pro soukromí, jež je případně s aplikací spojena;
 - b) přijali vhodná technická a organizační opatření s cílem zajistit ochranu soukromých údajů a soukromí;
 - c) určili osobu nebo skupinu osob odpovědných za přezkum posouzení a další vhodnosti technických a organizačních opatření k zajištění ochrany soukromých údajů a soukromí;
 - d) zpřístupnili posouzení příslušnému orgánu nejméně šest týdnů před zavedením aplikace;
 - e) jakmile bude k dispozici rámec pro posuzování dopadů na soukromí a ochranu údajů stanovený v bodě 4, prováděli výše uvedená ustanovení v souladu s tímto rámcem.

Bezpečnost informací

6. Členské státy by měly Komisi podpořit při určování aplikací, které mohou představovat hrozbu pro bezpečnost informací s důsledky pro širokou veřejnost. U těchto apli-

kací by měly členské státy zajistit, aby provozovatelé spolu s příslušnými vnitrostátními orgány a organizacemi občanské společnosti vyvinuli nové systémy nebo používali stávající systémy, například osvědčování nebo sebehodnocení provozovatele, s cílem prokázat, že s ohledem na posuzovaná rizika je zajištěna přiměřená úroveň bezpečnosti informací a ochrany soukromí.

Informování a transparentnost používání RFID

7. Aniž jsou dotčeny povinnosti správců údajů v souladu se směrnicemi 95/46/ES a 2002/58/ES, členské státy by měly zajistit, aby provozovatelé pro každou ze svých aplikací vypracovali a zveřejnili stručnou, přesnou a srozumitelnou informační politiku. Tato politika by měla zahrnovat přinejmenším:
- a) totožnost a adresu provozovatelů;
 - b) účel aplikace;
 - c) jaké údaje má aplikace zpracovávat, zejména v případě zpracování osobních údajů, a zda bude sledováno umístění etiket;
 - d) souhrn posouzení dopadů na soukromí a ochranu údajů;
 - e) pravděpodobná rizika pro soukromí (pokud existují) v souvislosti s používáním etiket v aplikaci a opatření, jež mohou jednotlivci přijmout ke zmírnění těchto rizik.
8. Členské státy by měly zajistit, aby provozovatelé přijali opatření k informování jednotlivců o přítomnosti čteček na základě společné evropské značky vypracované evropskými normalizačními organizacemi s podporou dotčených zúčastněných stran. Značka by měla udávat totožnost provozovatele a kontaktní místo, kde mohou jednotlivci obdržet informační politiku pro danou aplikaci.

Aplikace RFID používané v maloobchodu

9. Na základě společné evropské značky vypracované normalizačními organizacemi s podporou dotčených zúčastněných stran by provozovatelé měli jednotlivce informovat o přítomnosti etiket, jež jsou umístěny na výrobcích či v nich zabudovány.

10. Při posuzování dopadů na soukromí a ochranu údajů uvedeného v bodech 4 a 5 by provozovatel aplikace měl zejména určit, zda etikety umístěné na výrobcích či zabudované ve výrobcích, jež jsou prodávány spotřebitelům prostřednictvím maloobchodníků, kteří nejsou provozovateli dané aplikace, představují pravděpodobnou hrozbu pro soukromí nebo ochranu osobních údajů.
11. Maloobchodníci by měli v okamžiku prodeje deaktivovat nebo odstranit etikety používané v jejich aplikaci, ledaže spotřebitele poté, co byli informováni o politice uvedené v bodě 7, udělili souhlas se zachováním funkčnosti etiket. Deaktivací etiket se rozumí proces, který zastaví interakce etikety s jejím okolím, jež nevyžadují aktivní účast spotřebitele. Deaktivaci nebo odstranění etiket by měl maloobchodník provést pro spotřebitele neprodleně a zdarma. Spotřebitelé by měli být schopni ověřit, zda je deaktivace nebo odstranění účinné.
12. Bod 11 by se neměl použít v případě, dospěje-li posouzení dopadů na soukromí a ochranu údajů k závěru, že etikety, které jsou používány v maloobchodní aplikaci a které zůstanou po prodeji funkční, nepředstavují pravděpodobnou hrozbu pro soukromí nebo ochranu soukromých údajů. Maloobchodníci by však měli zdarma poskytnout snadné prostředky pro okamžitou či pozdější deaktivaci nebo odstranění těchto etiket.
13. Deaktivace nebo odstranění etiket neznamená omezení či zrušení právních povinností maloobchodníka nebo výrobce vůči spotřebiteli.
14. Body 11 a 12 platí pouze pro maloobchodníky, kteří jsou provozovateli aplikace.

Opatření k zvýšení informovanosti

15. Členské státy by měly ve spolupráci s odvětvím, Komisí a ostatními zúčastněnými stranami přijmout vhodná opatření s cílem informovat orgány veřejné správy a společnosti, zejména malé a střední podniky, a zvýšit jejich povědomí o možných přínosech a rizicích spojených s používáním technologie RFID. Zvláštní pozornost je nutno věnovat aspektům bezpečnosti informací a soukromí.
16. Členské státy by měly ve spolupráci s odvětvím, sdruženími občanské společnosti, Komisí a ostatními zúčastněnými

stranami určit a poskytnout příklady osvědčených postupů při zavádění aplikací RFID s cílem informovat širokou veřejnost a zvýšit její povědomí o této záležitosti. Měly by rovněž přijmout vhodná opatření, například rozsáhlé pilotní projekty, ke zvýšení informovanosti veřejnosti o technologii RFID, jejích přínosech, rizicích a o důsledcích jejího používání jako předpoklad pro širší přijetí této technologie.

Výzkum a vývoj

17. Členské státy by měly spolupracovat s odvětvím, příslušnými zúčastněnými stranami z občanské společnosti a s Komisí s cílem podnítit a podpořit zavedení zásady „konstrukčního návrhu nenarušujícího bezpečnost a soukromí“ v počáteční fázi vývoje aplikací RFID.

Následná opatření

18. Členské státy by měly přijmout veškerá nezbytná opatření s cílem upozornit na toto doporučení všechny zúčastněné strany, které se podílejí na navrhování a provozování aplikací RFID ve Společenství.
19. Členské státy by měly nejpozději do 24 měsíců od vyhlášení tohoto doporučení v *Úředním věstníku Evropské unie* Komisi informovat o opatřeních přijatých v reakci na toto doporučení.
20. Do tří let od vyhlášení tohoto doporučení v *Úředním věstníku Evropské unie* Komise předloží zprávu o provádění tohoto doporučení, jeho účinnosti a dopadu na provozovatele a spotřebitele, zejména s ohledem na opatření, jež jsou doporučena v bodech 9 až 14.

Určení

21. Toto doporučení je určeno členskými státním.

V Bruselu dne 12. května 2009.

Za Komisi
Viviane REDING
členka Komise