RECOMANDĂRI

COMISIE

RECOMANDAREA COMISIEI

din 12 mai 2009

privind aplicarea principiilor de respectare a vieții private și protecție a datelor în aplicațiile bazate pe identificarea prin radiofrecvență

[notificată cu numărul C(2009) 3200]

(2009/387/CE)

COMISIA COMUNITĂȚILOR EUROPENE,

având în vedere Tratatul de instituire a Comunității Europene, în special articolul 211,

după consultarea Autorității Europene pentru Protecția Datelor,

întrucât:

(1) Identificarea prin radiofrecvență (RFID) marchează o nouă evoluție a societății informaționale, în care obiectele dotate cu dispozitive microelectronice care permit prelucrarea automată a datelor vor deveni din ce în ce mai mult parte integrantă a vieții de zi cu zi.

(2) Tehnologia RFID este din ce în ce mai comună, devenind parte din viața cetățenilor într-o serie de domenii precum logistică [1], sănătate, transporturi publice, comerț cu ridicata, în special pentru o mai mare siguranță a produselor și o retragere mai rapidă a acestora, divertisment, muncă, taxare rutieră, gestionarea bagajelor și documente de călătorie.

(3) Tehnologia RFID are potențialul de a deveni un nou motor de creștere și ocupare a forței de muncă, aducând astfel o contribuție importantă la Strategia de la Lisabona, dat fiind că este foarte promițătoare din punct de vedere economic și poate genera noi oportunități de afaceri, reduceri ale costurilor și creșteri ale eficienței, în special în domeniul combaterii contrafacerilor, al gestionării deșeurilor electronice și a materialelor periculoase și al reciclării produselor la sfârșitul vieții utile.

(4) Tehnologia RFID permite prelucrarea datelor, inclusiv a celor cu caracter personal, la distanțe scurte, fără un contact fizic sau o interacțiune vizibilă între cititor sau gravor și etichetă, astfel că interacțiunea se poate produce fără ca persoana în cauză să fie conștientă de acest lucru.

(5) Aplicațiile RFID oferă posibilitatea de a prelucra date referitoare la o persoană fizică identificată sau identificabilă în mod direct sau indirect. Ele permit prelucrarea datelor personale stocate pe etichetă precum numele, data nașterii sau adresa persoanei, datele biometrice sau date care conectează numărul unui element RFID specific la date cu caracter personal stocate într-un alt loc din sistem. În plus, există posibilitatea ca această tehnologie să fie utilizată pentru monitorizarea persoanelor fizice prin intermediul unuia sau al mai multor articole aflate în posesia lor care poartă un număr RFID.

(6) Întrucât tehnologia RFID este atât ubicuă, cât și practic invizibilă, este necesar ca în dezvoltarea acesteia să se acorde o atenție specială aspectelor legate de respectarea vieții private și de protecția datelor. Prin urmare, în aplicațiile RFID trebuie integrate caracteristici care să asigure respectarea vieții private și securitatea informațiilor înainte de difuzarea lor la scară largă (principiul „securității și respectării vieții private din momentul proiectării").

(7) Tehnologia RFID va putea produce numeroase beneficii economice și sociale, cu condiția să se prevadă măsuri eficiente de protecție a datelor, a vieții private și a principiilor etice asociate care se află în centrul dezbaterii privind acceptarea RFID de către publicul larg.

(8) Statele membre și părțile interesate trebuie să facă eforturi suplimentare, în special în această fază inițială a implementării RFID, pentru a asigura monitorizarea aplicațiilor RFID și respectarea drepturilor și a libertăților individuale.

[1] COM(2007) 607 final.

(9) Comunicarea Comisiei din 15 martie 2007 cu titlul „Identificarea prin radiofrecvență (RFID) în Europa: etape în direcția elaborării unui cadru strategic" [1] anunța publicarea uneia sau a mai multor recomandări ale Comisiei care vor cuprinde clarificări și indicații privind aspectele legate de protecția datelor și a vieții private aferente aplicațiilor RFID.

(10) Drepturile și obligațiile privind protecția datelor cu caracter personal și libera circulație a acestora prevăzute de Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date [2] și de Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice) [3] sunt pe deplin aplicabile utilizării de aplicații RFID care prelucrează date cu caracter personal.

(11) În dezvoltarea aplicațiilor RFID trebuie aplicate principiile prevăzute în Directiva 1999/5/CE a Parlamentului European și a Consiliului din 9 martie 1999 privind echipamentele hertziene și echipamentele terminale de telecomunicații și recunoașterea reciprocă a conformității acestora [4].

(12) Avizul Autorității Europene pentru Protecția Datelor [5] oferă indicații privind modalitatea de gestionare a produselor care conțin etichete și sunt furnizate persoanelor fizice și subliniază necesitatea efectuării de evaluări ale impactului asupra vieții private și a securității pentru a identifica și dezvolta „cele mai bune tehnici disponibile" în vederea garantării respectării vieții private și a securității de către sistemele RFID.

(13) Operatorii aplicațiilor RFID trebuie să ia toate măsurile rezonabile pentru a se asigura că datele nu se referă la o persoană fizică identificată sau identificabilă prin niciun mijloc care ar putea fi utilizat de către operatorul însuși sau de către o altă persoană, cu excepția cazului în care datele sunt prelucrate cu respectarea principiilor și a normelor de drept aplicabile în materie de protecție a datelor.

(14) Comunicarea Comisiei din 2 mai 2007 intitulată „Promovarea protecției datelor prin intermediul tehnologiilor de protecție a vieții private" [6] prevede acțiuni concrete în vederea atingerii obiectivului de limitare a prelucrării datelor cu caracter personal și de utilizare, pe cât posibil, a datelor anonime sau sub pseudonim, sprijinind dezvoltarea acestor tehnologii și utilizarea lor de către responsabilii de prelucrarea datelor și de către persoanele fizice.

(15) Comunicarea Comisiei din 31 mai 2006 intitulată „O strategie pentru o societate informațională sigură – Dialog, parteneriat și responsabilizare" [7] recunoaște faptul că diversitatea, deschiderea, interoperabilitatea, ușurința utilizării și concurența constituie motoarele principale ale unei societăți informaționale sigure, subliniază rolul statelor membre și al administrațiilor publice în îmbunătățirea nivelului de informare și în promovarea bunelor practici în materie de securitate și invită părțile interesate din sectorul privat să ia inițiative pentru elaborarea unor sisteme abordabile de certificare a securității produselor, proceselor și serviciilor care să răspundă unor nevoi specifice ale UE, în special cu privire la respectarea vieții private.

(16) Rezoluția Consiliului din 22 martie 2007 cu privire la o strategie pentru o societate informațională sigură în Europa [8] invită statele membre să acorde atenția care se cuvine necesității de a preveni și de a combate amenințările noi sau existente la adresa securității rețelelor de comunicații electronice.

(17) Un cadru elaborat la nivel comunitar pentru realizarea de evaluări ale impactului asupra protecției datelor și a vieții private va asigura aplicarea uniformă a prevederilor prezentei recomandări în toate statele membre. Elaborarea unui astfel de cadru trebuie să se bazeze pe practicile existente și pe experiența acumulată în statele membre, în țările terțe și cu ocazia lucrărilor efectuate de Agenția Europeană pentru Securitatea Rețelelor Informatice și a Datelor (ENISA) [9].

(18) Comisia va asigura elaborarea unor linii directoare la nivel comunitar cu privire la managementul securității informațiilor pentru aplicațiile RFID, pe baza practicilor existente și a experienței acumulate în statele membre și în țările terțe. Statele membre trebuie să contribuie la acest proces și să încurajeze participarea entităților private și a autorităților publice.

(19) O evaluare a impactului asupra protecției datelor și a vieții private efectuată de operator înaintea implementării unei aplicații RFID va oferi informațiile necesare pentru luarea unor măsuri adecvate de protecție. Aceste măsuri vor trebui monitorizate și revizuite pe parcursul întregului ciclu de viață al aplicației RFID.

(20) În sectorul comerțului cu amănuntul, o evaluare a impactului asupra protecției datelor și a vieții private al produselor conținând etichete care sunt vândute consumatorilor va oferi informațiile necesare pentru a stabili existența unui potențial risc la adresa protecției datelor personale sau a vieții private.

[1] COM(2007) 96 final.
[2] JO L 281, 23.11.1995, p. 31.
[3] JO L 201, 31.7.2002, p. 37.
[4] JO L 91, 7.4.1999, p. 10.
[5] JO C 101, 23.4.2008, p. 1.
[6] COM(2007) 228 final.
[7] COM(2006) 251 final.
[8] JO C 68, 24.3.2007, p. 1.
[9] Articolul 2 alineatul (1) din Regulamentul (CE) nr. 460/2004 al Parlamentului European și al Consiliului (JO L 77, 13.3.2004, p. 1).

(21) Utilizarea unor standarde internaționale, cum sunt cele elaborate de Organizația Internațională pentru Standardizare (ISO), a unor coduri de conduită și a celor mai bune practici conforme cadrului de reglementare comunitar poate contribui la adoptarea unor măsuri de securitate a informațiilor și de respectare a vieții private pe durata întregului proces de afaceri bazat pe RFID.

(22) Aplicațiile RFID cu efecte asupra publicului larg, cum sunt biletele electronice din transportul public, impun adoptarea unor măsuri adecvate de protecție. Aplicațiile RFID care afectează persoanele fizice, de exemplu prin prelucrarea datelor biometrice de identificare sau a datelor de sănătate, sunt în mod special sensibile din punct de vedere al securității informațiilor și al protecției vieții private, așadar necesită o atenție specială.

(23) Societatea în ansamblul său trebuie să cunoască drepturile și obligațiile aplicabile în contextul utilizării aplicațiilor RFID. Părțile implicate în implementarea tehnologiei au, prin urmare, responsabilitatea de a oferi persoanelor informații în legătură cu utilizarea acestor aplicații.

(24) Îmbunătățirea nivelului de informare al publicului și al întreprinderilor mici și mijlocii (IMM) cu privire la caracteristicile și funcțiile RFID va permite acestei tehnologii să genereze beneficiile economice promise, reducând în același timp riscurile de a fi utilizată în detrimentul interesului public și sporind prin aceasta acceptabilitatea sa.

(25) Comisia va contribui la implementarea prezentei recomandări direct și indirect, facilitând dialogul și cooperarea între părțile interesate, în special prin intermediul programului-cadru pentru competitivitate și inovare instituit prin Decizia nr. 1639/2006/CE a Parlamentului European și a Consiliului [1] și al celui de-al șaptelea program-cadru pentru cercetare (PC7) instituit prin Decizia nr. 1982/2006/CE a Parlamentului European și a Consiliului [2].

(26) Cercetarea și dezvoltarea în domeniul tehnologiilor rentabile de îmbunătățire a protecției vieții private și al tehnologiilor de securizare a informațiilor sunt esențiale la nivel comunitar pentru a promova o mai largă adoptare a acestora în condiții acceptabile.

(27) Prezenta recomandare respectă drepturile fundamentale și principiile recunoscute în special de Carta Drepturilor Fundamentale a Uniunii Europene. Recomandarea caută să asigure în principal respectarea deplină a vieții private și a vieții de familie și protecția datelor cu caracter personal,

[1] JO L 310, 9.11.2006, p. 15.
[2] JO L 412, 30.12.2006, p. 1.

RECOMANDĂ:

Domeniul de aplicare

1. Prezenta recomandare oferă statelor membre indicații cu privire la conceperea și exploatarea aplicațiilor RFID într-un mod legal, etic, acceptabil din punct de vedere social și politic, cu respectarea dreptului la viață privată și asigurând protecția datelor cu caracter personal.

2. Prezenta recomandare oferă indicații cu privire la măsurile care trebuie luate la implementarea aplicațiilor RFID pentru a se asigura respectarea legislației naționale de transpunere a Directivelor 95/46/CE, 1999/5/CE și 2002/58/CE, după caz.

Definiții

3. În sensul prezentei recomandări, se aplică definițiile stabilite în Directiva 95/46/CE. De asemenea, se aplică definițiile următoare:

(a) „identificare prin radiofrecvență (RFID)" înseamnă utilizarea undelor electromagnetice sau a unui cuplaj de câmp reactiv în porțiunea de frecvențe radio a spectrului pentru comunicarea bidirecțională cu o etichetă printr-o serie de dispozitive de modulare și codare pentru a citi în mod univoc identitatea unei etichete de radiofrecvență sau alte date stocate pe etichetă;

(b) „etichetă RFID" sau „etichetă" înseamnă fie un dispozitiv RFID care are capacitatea de a produce un semnal radio, fie un dispozitiv RFID care recuplează, retrodifuzează sau reflectă (în funcție de tipul dispozitivului) și modulează un semnal electronic purtător (*carrier signal*) primit de la un cititor sau un gravor;

(c) „cititor sau gravor RFID" sau „cititor" înseamnă un dispozitiv fix sau mobil de captare și identificare a datelor care utilizează o undă electromagnetică de frecvență radio sau un cuplaj de câmp reactiv pentru a stimula și a produce un răspuns de date modulate de la o etichetă sau un grup de etichete;

(d) „aplicație RFID" sau „aplicație" înseamnă o aplicație care prelucrează date prin utilizarea etichetelor și a cititoarelor și care are la bază un sistem back-end și o infrastructură de comunicații în rețea;

(e) „operator al aplicației RFID" sau „operator" înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau orice alt organism care, singur sau împreună cu alții, stabilește scopurile și mijloacele de exploatare a unei aplicații, inclusiv responsabilii de prelucrarea datelor cu caracter personal care utilizează o aplicație RFID;

(f) „securitatea informațiilor” înseamnă asigurarea confidențialității, a integrității și a disponibilității informațiilor;

(g) „monitorizare” înseamnă orice activitate desfășurată în scopul detectării, observării, copierii sau înregistrării poziției, deplasării, activității sau stării unei persoane.

Evaluarea impactului asupra protecției datelor și a vieții private

4. Statele membre se asigură că sectorul, în colaborare cu părțile interesate din cadrul societății civile, elaborează un cadru pentru evaluarea impactului asupra protecției datelor și a vieții private. Acest cadru trebuie înaintat spre aprobare Grupului de lucru „articolul 29” pentru protecția datelor în termen de 12 luni de la publicarea prezentei recomandări în *Jurnalul Oficial al Uniunii Europene*.

5. Statele membre se asigură că operatorii, fără a aduce atingere celorlalte obligații care le revin în temeiul Directivei 95/46/CE:

(a) efectuează o evaluare a efectelor implementării aplicației asupra protecției datelor cu caracter personal și a vieții private, inclusiv a posibilității ca aplicația să fie utilizată pentru monitorizarea unei persoane. Nivelul detaliilor acestei evaluări trebuie să fie adecvat în raport cu riscurile potențiale la adresa vieții private asociate aplicației;

(b) iau măsurile tehnice și organizaționale corespunzătoare pentru a asigura protecția datelor cu caracter personal și a vieții private;

(c) desemnează o persoană sau un grup de persoane responsabile de revizuirea evaluărilor și examinarea menținerii caracterului adecvat al măsurilor tehnice și organizaționale luate pentru a asigura protecția datelor cu caracter personal și a vieții private;

(d) pun evaluarea la dispoziția autorității competente cu cel puțin șase săptămâni înainte de implementarea aplicației;

(e) după instituirea cadrului pentru evaluarea impactului asupra protecției datelor și a vieții private menționat la punctul 4, aplică prevederile de mai sus în conformitate cu acesta.

Securitatea informațiilor

6. Statele membre trebuie să sprijine Comisia la identificarea aplicațiilor care pot prezenta riscuri legate de securitatea informațiilor cu implicații pentru publicul larg. În cazul acestor aplicații, statele membre trebuie să se asigure că operatorii, împreună cu autoritățile naționale competente și cu organizațiile societății civile, elaborează noi sisteme sau aplică sisteme existente precum certificarea sau autoevaluarea operatorului pentru a demonstra că nivelul de securitate a informațiilor și de protecție a vieții private este corespunzător în raport cu riscurile evaluate.

Informații și transparență în legătură cu utilizarea RFID

7. Fără a aduce atingere obligațiilor care le revin responsabililor de prelucrare a datelor în temeiul Directivelor 95/46/CE și 2002/58/CE, statele membre trebuie să se asigure că operatorii elaborează și publică o politică de informare concisă, fiabilă și inteligibilă pentru fiecare aplicație. Această politică trebuie să includă cel puțin următoarele:

(a) identitatea și adresa operatorilor;

(b) scopul aplicației;

(c) datele care urmează să fie prelucrate prin aplicație, în special dacă este vorba de prelucrarea unor date cu caracter personal, precizând dacă locația etichetelor va face obiectul monitorizării;

(d) un rezumat al evaluării impactului asupra protecției datelor și a vieții private;

(e) riscurile probabile pe care utilizarea etichetelor în aplicație le prezintă pentru viața privată și măsurile pe care persoanele le pot lua pentru limitarea acestora.

8. Statele membre trebuie să se asigure că operatorii iau măsuri pentru informarea persoanelor în legătură cu prezența cititoarelor prin intermediul unui semn european comun, dezvoltat de organizațiile europene de standardizare cu sprijinul părților interesate. Semnul trebuie să includă identitatea operatorului și un punct de contact de unde persoanele pot obține politica de informare aferentă aplicației.

Aplicații RFID utilizate în comerțul cu amănuntul

9. Prin intermediul unui semn european comun, dezvoltat de organizațiile europene de standardizare cu sprijinul părților interesate, operatorii trebuie să informeze persoanele în legătură cu prezența etichetelor aplicate pe produse sau integrate în acestea.

10. În momentul realizării evaluării impactului asupra protecției datelor și a vieții private menționate la punctele 4 și 5, operatorul unei aplicații trebuie să stabilească cu precizie dacă etichetele aplicate sau integrate în produse vândute consumatorilor de către comercianți cu amănuntul care nu sunt operatori ale aplicației respective prezintă un risc potențial la adresa protecției vieții private sau a datelor cu caracter personal.

11. Comercianții cu amănuntul trebuie să dezactiveze sau să înlăture la punctul de vânzare etichetele utilizate în aplicația lor, cu excepția cazului în care consumatorii, după ce au fost informați cu privire la politica menționată la punctul 7, acceptă ca etichetele să rămână operaționale. Dezactivarea etichetelor trebuie înțeleasă ca fiind orice proces care întrerupe interacțiunile unei etichete cu mediul său fără a necesita participarea activă a consumatorului. Dezactivarea sau înlăturarea etichetelor de către comerciantul cu amănuntul trebuie efectuată imediat și gratuit pentru consumator. Consumatorii trebuie să aibă posibilitatea de a verifica dacă dezactivarea sau înlăturarea au fost efectiv realizate.

12. Punctul 11 nu trebuie să se aplice atunci când din evaluarea impactului asupra protecției datelor și a vieții private reiese că etichetele care sunt utilizate într-o aplicație vândută cu amănuntul și care rămân operaționale dincolo de punctul de vânzare nu prezintă un risc potențial la adresa protecției datelor personale sau a vieții private. Cu toate acestea, comercianții cu amănuntul trebuie să pună la dispoziție în mod gratuit un mijloc accesibil de dezactivare sau înlăturare, imediat sau ulterior, a acestor etichete.

13. Dezactivarea sau înlăturarea etichetelor nu trebuie să atragă după sine reducerea sau încetarea obligațiilor legale ale comerciantului cu amănuntul sau ale producătorului față de consumator.

14. Punctele 11 și 12 trebuie să se aplice numai comercianților cu amănuntul care sunt operatori.

Acțiuni de sensibilizare

15. Statele membre, în colaborare cu sectorul, Comisia și alte părți interesate, trebuie să ia măsurile adecvate pentru informarea și sensibilizarea autorităților publice și a societăților, în special a IMM-urilor, cu privire la beneficiile și riscurile potențiale asociate utilizării tehnologiei RFID. Este necesar să se acorde o atenție specială aspectelor legate de securitatea informațiilor și de respectarea vieții private.

16. Statele membre, în colaborare cu sectorul, asociațiile societății civile, Comisia și alte părți interesate, trebuie să identifice și să ofere exemple de bune practici pentru implementarea aplicațiilor RFID pentru a informa și a sensibiliza publicul larg. Ele trebuie, de asemenea, să ia măsuri adecvate, cum ar fi proiecte-pilot de amploare, pentru creșterea nivelului de informare cu privire la tehnologia RFID și la beneficiile, riscurile și implicațiile utilizării ei, aceasta fiind o condiție prealabilă pentru adoptarea mai largă a tehnologiei.

Cercetare și dezvoltare

17. Statele membre trebuie să coopereze cu sectorul, cu părțile interesate ale societății civile și cu Comisia pentru a stimula și a sprijini introducerea principiului de „securitate și respectare a vieții private din momentul proiectării” într-o fază inițială a dezvoltării aplicațiilor RFID.

Acțiuni ulterioare

18. Statele membre trebuie să ia toate măsurile necesare pentru a aduce prezenta recomandare la cunoștința tuturor părților interesate care sunt implicate în proiectarea și exploatarea aplicațiilor RFID în Comunitate.

19. Statele membre trebuie să informeze Comisia în termen de cel mult 24 de luni de la publicarea prezentei recomandări în *Jurnalul Oficial al Uniunii Europene* cu privire la măsurile luate ca reacție la aceasta.

20. În termen de trei ani de la publicarea prezentei recomandări în *Jurnalul Oficial al Uniunii Europene*, Comisia va furniza un raport privind implementarea acesteia, eficacitatea și impactul său asupra operatorilor și a consumatorilor, în special în ceea ce privește măsurile recomandate la punctele 9-14.

Destinatari

21. Prezenta recomandare se adresează statelor membre.

Adoptată la Bruxelles, 12 mai 2009.

Pentru Comisie

Viviane REDING

Membru al Comisiei