GRUPUL DE LUCRU ÎN MATERIE DE PROTECȚIA DATELOR PREVĂZUT LA ARTICOLUL 29

00066/10/RO
GL 175

# Avizul 5/2010 privind o propunere din partea industriei pentru un cadru de evaluare a impactului asupra protecției datelor și a vieții private în cazul aplicațiilor RFID

**Adoptat la 13 iulie 2010**

**Cuprins**

# 1 Context

## 1.1 Introducere

La 12 mai, Comisia Europeană a emis o recomandare privind aplicarea principiilor de respectare a vieții private și protecție a datelor în aplicațiile bazate pe identificarea prin radiofrecvență[1].

Punctul 4 din această recomandare prevede că *„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 în materie de protecția datelor, prevăzut la„articolul 29" în termen de 12 luni de la publicarea prezentei recomandări în Jurnalul Oficial al Uniunii Europene" (sublinierea noastră).*

Conform recomandării, după definirea acestui cadru pentru evaluarea impactului asupra protecției datelor și a vieții private, statele membre ar trebui să se asigure că operatorii RFID realizează o evaluare a impactului asupra protecției datelor și a vieții private (PIA) în cazul aplicațiilor RFID înainte de implementarea acestora. De asemenea, statele membre trebuie să se asigure că operatorii RFID vor pune rapoartele PIA rezultate la dispoziția autorității competente (respectiv, APD).

În iulie 2009, un „grup de lucru pentru RFID" informal, coordonat de către reprezentanți ai industriei, a început să lucreze la definirea unui cadru de protecție a datelor și a vieții private (PIA), organizând totodată reuniuni periodice cu părțile interesate, inclusiv cu grupuri ale consumatorilor, organisme de standardizare și cadre didactice universitare. La data de 31 martie 2010, reprezentanții industriei au înaintat o propunere de cadru pentru evaluarea impactului asupra protecției datelor și a vieții private grupului de lucru 29 spre aprobare. **Acest aviz reprezintă răspunsul oficial al grupului de lucru la propunerea în cauză.**

În cele ce urmează, „recomandarea privind RFID" se referă la recomandarea Comisiei Europene privind aplicarea principiilor de respectare a vieții private și protecție a datelor în aplicațiile bazate pe identificarea prin radiofrecvență, publicată la 12 mai 2009. „Cadrul propus" sau, pur și simplu, „cadrul" se referă la cadrul de evaluare a impactului asupra protecției datelor și a vieții private în cazul aplicațiilor RFID, transmis grupului de lucru 29 la data de 31 martie 2010 și reprodus în apendicele la prezentul aviz.

## 1.2 RFID și protecția datelor

În ianuarie 2005, grupul de lucru a adoptat un *document de lucru*[2] *privind aspectele legate de protecția datelor conexe tehnologiei RFID* (GL 105), care recunoaște avantajele evidente oferite de tehnologia RFID, însă subliniază și potențialele motive de îngrijorare din domeniul protecției datelor, care apar, în special, din cauza *„posibilității întreprinderilor și guvernelor de a utiliza tehnologia RFID pentru a se amesteca în sfera privată a persoanelor fizice"*. Acest document a evidențiat faptul că *„abilitatea de a*

[1] http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf
[2] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf

*colecta pe furiș o varietate de date legate de aceeași persoană, de a urmări persoanele fizice în timp ce acestea se deplasează în locuri publice (aeroporturi, gări, magazine), de a îmbunătăți profilurile firmelor prin monitorizarea comportamentului consumatorilor în magazine, de a citi detaliile legate de articolele de îmbrăcăminte și accesoriile purtate sau medicamentele deținute de către clienți reprezintă exemple de utilizare a tehnologiei RFID care suscită motive de îngrijorare legate de respectarea vieții private*".

Acest document de lucru a fost pus la dispoziția publicului spre consultare. Rezultatul acestui proces a fost rezumat într-un document (GL 111)[3] publicat de către grupul de lucru în septembrie 2005. Rezultatele au indicat că, deși „*majoritatea universităților, grupurilor de reflecție, persoanelor fizice și întreprinderilor care oferă soluții de securitate au sugerat necesitatea unor anumite orientări suplimentare din partea grupului de lucru 29"*, iar unii au sugerat *„completarea directivei privind protecția datelor cu norme specifice pentru RFID"*, industria a susținut o *„abordare bazată pe autoreglementare"*.

În acest context global și în colaborare cu părțile interesate, inclusiv cu reprezentanți ai industriei RFID, organizații pentru drepturile consumatorilor și protecția datelor, Comisia Europeană a preluat inițiativa elaborării unei recomandări[4] „*privind aplicarea principiilor de respectare a vieții private și protecție a datelor în aplicațiile bazate pe identificarea prin radiofrecvență"*", cu scopul de a oferi „*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"*."

Această recomandare, publicată în mai 2009, include un important element de noutate: ea impune operatorului RFID să realizeze o „evaluare a impactului asupra protecției datelor și a vieții private"" înainte de implementarea unei aplicații RFID și să pună rezultatele acesteia la dispoziția autorității competente. Această nouă abordare, care vine în completarea cadrului de reglementare existent, prevăzut în Directiva privind protecția datelor și în Directiva privind protecția vieții private în mediul electronic, oferă industriei ocazia de a demonstra potențialul autoreglementării în calitate de instrument complementar, flexibil și eficient pentru cadrul juridic al UE, în contextul unui peisaj tehnologic într-o schimbare accelerată. Grupul de lucru sprijină[5] *„realizarea unor evaluări ale impactului asupra vieții private, în special în cazul anumitor operațiuni de prelucrare a datelor considerate ca prezentând riscuri specifice pentru drepturile și libertățile persoanelor vizate"*. De asemenea, acesta este de părere că succesul sau eșecul acestei abordări este de natură fie să deschidă calea pentru utilizarea evaluărilor PIA și în alte domenii, fie să determine o abordare de reglementare mai accentuată.

Recomandarea privind RFID este, de asemenea, elaborată pentru a promova „*informațiile și transparența privind utilizarea RFID*", în special prin intermediul stabilirii unui *„semn european comun dezvoltat de către organizațiile europene de standardizare, cu sprijinul părților interesate vizate",* cu scopul de a

---

3 *„Rezultatele consultării publice cu privire la documentul de lucru 105 al grupului de lucru prevăzut la articolul 29 privind aspectele legate de protecția datelor conexe tehnologiei RFID"*, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp111_en.pdf

4 http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf

5 A se vedea „Viitorul respectării vieții private: contribuția comună la consultarea Comisiei Europene privind cadrul juridic pentru dreptul fundamental la protecția datelor cu caracter personal", GL 168, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp168_en.pdf

*„informa persoanele în legătură cu prezența cititorilor”*. O astfel de inițiativă beneficiază de sprijinul deplin al grupului de lucru.

Cu toate că recomandarea privind RFID se referă, în mod explicit, la Directiva 95/46/CE, în unele situații, aceasta se abate de la terminologia utilizată în mod tradițional în legislația privind protecția datelor, în special atunci când face referire la „persoane”, „indivizi” sau „utilizatori”. Pentru a evita ambiguitatea, în acest aviz se va utiliza cuvântul „persoană” pentru a desemna o persoană fizică, la fel ca în articolul 2 din Directiva 95/46/CE, în timp ce cuvintele „Utilizator”” și „Individ”, scrise cu inițială majusculă, își vor păstra sensul pe care îl au în cadrul recomandării privind RFID. În special, cuvântul „persoană” poate fi utilizat pentru a desemna, în sens larg, atât „Utilizatori”, cât și „Indivizi”, care reprezintă, în alte situații, categorii de persoane distincte conform definițiilor stabilite la punctul 3 din recomandarea privind RFID și repetate în cadrul propus. Pentru a asigura coerența cu recomandarea privind RFID, în prezentul aviz se va face, de asemenea, referire la „operatori RFID” în locul „operatorilor de date”, deși acești termeni nu sunt absolut echivalenți.

În noiembrie 2009, organismele legislative europene au modificat Directiva privind protecția vieții private în mediul electronic[6] și au făcut referire, în mod explicit, la tehnologia RFID. În considerentul 56 din Directiva 2009/136/CE, acestea recunosc atât că *„larga utilizare a unor astfel de tehnologii poate să aducă beneficii economice și sociale considerabile și, astfel, să contribuie semnificativ la piața internă dacă utilizarea acestora este acceptată de către cetățeni”*, cât și că *„pentru a se realiza acest lucru, este necesar să se garanteze că toate drepturile fundamentale ale persoanelor, inclusiv dreptul la confidențialitate și la protecția datelor, sunt respectate”*. Mai departe, organismele legislative adaugă că *„atunci când astfel de dispozitive sunt conectate cu rețele de comunicații electronice destinate publicului sau când utilizează serviciile de comunicații electronice ca infrastructură de bază, trebuie aplicate dispozițiile relevante din Directiva 2002/58/CE (directiva asupra confidențialității și comunicațiilor electronice), inclusiv cele privind datele legate de securitate, trafic și localizare și cele privind confidențialitatea”*. În consecință, domeniul de aplicare al directivei privind protecția vieții private în mediul electronic (definit la articolul 3) a fost revizuit pentru a include *„rețelele publice de comunicații care presupun colectarea de date și dispozitive de identificare”*.

## *1.3 Obiectivele cadrului PIA*

Prin intermediul recomandării privind RFID, Comisia Europeană a creat un proces PIA care are ca scop obținerea unei serii de beneficii:

- În primul rând, o evaluare PIA trebuie să favorizeze „respectarea vieții private din momentul proiectării”, sprijinind operatorii de date în vederea abordării protecției datelor și a vieții private înainte de implementarea unui serviciu sau unui produs. De pe urma acestui fapt vor beneficia nu doar indivizii, ci și operatorii de date, datorită evitării costurilor semnificative (și a soluțiilor

[6] Directiva 2009/136/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009 de modificare a Directivei 2002/22/CE privind serviciul universal și drepturile utilizatorilor cu privire la rețelele și serviciile de comunicații electronice, a Directivei 2002/58/CE privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice și a Regulamentului (CE) nr. 2006/2004 privind cooperarea dintre autoritățile naționale însărcinate să asigure aplicarea legislației în materie de protecție a consumatorului.

adesea nesatisfăcătoare) care apar deseori atunci când funcțiile de respectare a vieții private trebuie să „se plieze” pe un produs deja implementat.

- În al doilea rând, o evaluare PIA trebuie să sprijine operatorii de date în vederea eliminării riscurilor legate de protecția datelor și a vieții private într-un mod cuprinzător. Într-adevăr, PIA se numără printre instrumentele care ajută la evaluarea riscurilor pentru viața privată, la identificarea de măsuri tehnice și organizaționale pentru a proteja datele cu caracter personal împotriva dezvăluirii sau accesării neautorizate și la îndeplinirea altor obligații de securitate stabilite la articolul 17 din Directiva privind protecția datelor și la articolul 4 din Directiva 2002/58 modificată. De asemenea, acest proces oferă o ocazie de a reduce incertitudinea juridică și de a evita pierderea încrederii publicului, care altfel ar putea împovăra operatorul de date atunci când problemele legate de protecția datelor nu sunt soluționate în mod corespunzător.

- În sfârșit, evaluările PIA pot sprijini atât operatorii de date, cât și autoritățile de protecție a datelor pentru a dobândi mai multe informații despre aspecte ale aplicațiilor RFID care vizează respectarea vieții private și protecția datelor. Realizarea unei evaluări PIA trebuie să ajute operatorii de date să înțeleagă și să pună în aplicare principiile stabilite prin Directiva 95/46/CE, prin Directiva 2002/58/CE recent modificată și prin recomandarea privind RFID. Informațiile din evaluările PIA pot ajuta autoritățile de protecție a datelor (APD) să identifice bunele practici în ceea ce privește modalitatea de punere în aplicare a protecției datelor de către industrie, iar, în acele state membre care impun verificarea prealabilă a (anumitor sau tuturor) aplicațiilor RFID, pot simplifica procesul atât în cazul APD, cât și în cel al operatorilor de date[7].

În plus, grupul de lucru consideră că dezvoltarea evaluărilor PIA este un factor care contribuie la competitivitatea industriei europene a RFID prin stimularea abordărilor inovatoare în scopul rezolvării problemelor legate de respectarea vieții private și protecția datelor prin intermediul tehnologiilor precum anonimizarea, dezactivarea parțială a etichetelor, criptografia simplă etc.

Deși cadrul PIA prevăzut în recomandare este destinat promovării „securității și respectării vieții private din momentul proiectării” prin analizarea aplicațiilor RFID înainte de implementarea lor, la ora actuală există numeroase aplicații RFID deja implementate. Grupul de lucru speră că părțile interesate vor valorifica această experiență și vor profita de ocazie pentru a crea instrumente de evaluare care să poată fi utilizate în cazul aplicațiilor RFID existente.

## *1.4 Rezumatul cadrului propus*

Cadrul propus clasifică mai întâi o aplicație RFID în patru niveluri posibile. Aplicațiile de „nivel 0”, care includ, în principal, aplicațiile RFID ce nu prelucrează date cu caracter personal și în care etichetele sunt manipulate exclusiv de către Utilizatori, sunt excluse dintr-o evaluare PIA. Deși există posibilitatea ca termenul „Utilizator” să facă referire și la angajați, definiția nivelului 0 nu poate fi înțeleasă ca

[7] În acest context, punctul 5 litera d din recomandarea privind RFID prevede că operatorii, fără a aduce atingere celorlalte obligații ale acestora în conformitate cu Directiva 95/46/CE, trebuie să pună evaluarea la dispoziția autorității competente cu cel puțin șase săptămâni înainte de implementarea aplicației. Modul în care PIA trebuie pusă la dispoziție (de exemplu, la cerere sau nu) se stabilește de către autoritățile APD naționale. În special, pot fi avute în vedere riscurile asociate aplicației, precum și alți factori cum ar fi prezența unui responsabil pentru protecția datelor.

incluzând o aplicație ce ar fi destinată monitorizării angajaților, având în vedere că o asemenea monitorizare ar necesita stocarea datelor cu caracter personal într-o componentă a aplicației. În consecință, grupul de lucru este de acord că nu există probabilitatea ca excluderea „aplicațiilor de nivel 0" din procesul PIA să aducă prejudicii obiectivelor privind protecția datelor și respectarea vieții private.

Aplicațiile de nivel 1 includ aplicațiile în care nu se prelucrează date cu caracter personal, deși etichetele sunt deținute de Indivizi. Aplicațiile de nivel 2 reprezintă acele aplicații care prelucrează date cu caracter personal, dar în care etichetele în sine nu conțin date cu caracter personal. În sfârșit, aplicațiile de nivel 3 sunt aplicațiile în care etichetele conțin date cu caracter personal. Așa cum se subliniază în secțiunea 2.4 de mai jos, utilizarea termenilor „date cu caracter personal" este, într-o anumită măsură, ambiguă în cadrul propus atunci când face referire la informațiile incluse în etichetă.

În cazul în care se stabilește că nivelul aplicației RFID este de 1 sau mai mare, operatorul RFID are obligația de a realiza o analiză a aplicației structurată în patru părți, cu un nivel de detaliere proporțional cu implicațiile identificate în ceea ce privește respectarea vieții private și protecția datelor. Prima parte este destinată descrierii aplicației RFID. Cea de a doua parte permite evidențierea măsurilor de control și securitate. Partea a treia abordează informațiile și drepturile utilizatorului. În ultima parte a cadrului PIA propus, operatorul RFID are obligația de a concluziona dacă aplicația RFID este sau nu gata de a fi implementată. Ca urmare a procesului PIA, operatorul RFID va elabora un raport PIA care va fi pus la dispoziția autorității competente.

Autorii cadrului propus preconizează că, din cauza unor nevoi specifice sectorului, este posibil ca industria să transpună cadrul în „șabloane PIA" specifice pentru a facilita punerea în aplicare. Astfel, „raportul PIA" va fi constituit pe baza șablonului specific sectorului în locul unui cadru mai general.

# 2 Analiză

Grupul de lucru recunoaște activitatea semnificativă desfășurată de autorii cadrului propus și subscrie la obiectivele principale ale acestuia, evidențiate în secțiunile introductive.

Deși planul global al cadrului propus nu ridică întrebări deosebite, grupul de lucru a identificat 3 motive de îngrijorare critice în conținutul acestuia, precum și anumite observații care sunt detaliate în cele ce urmează.

## *2.1 Evaluarea riscurilor*

Secțiunea introductivă a cadrului propus prevede în mod clar că *„procesul PIA are ca scop depistarea riscurilor pentru viața privată asociate cu o aplicație RFID […] și evaluarea măsurilor luate pentru a elimina riscurile respective"*. **Cu toate acestea, acest principiu de bază al procesului PIA lipsește din conținutul cadrului propus.**

Într-adevăr, deși cadrul propus conține trimiteri izolate la evaluarea riscurilor (în principal, în părțile sale introductive), nicio secțiune nu impune în mod explicit operatorului RFID să identifice sau să *„depisteze riscurile pentru viața privată asociate cu o aplicație RFID"*. În consecință, *„evaluarea măsurilor luate pentru a elimina riscurile respective"* nu este posibilă. În schimb, cadrul propus impune operatorului

RFID doar să întocmească o listă a diferitelor măsuri de protecție și controale care au fost puse în aplicare pentru a proteja viața privată și datele cu caracter personal în aplicația RFID. Acest lucru nu poate fi considerat o metodă satisfăcătoare de a oferi operatorului RFID sau autorității competente un nivel rezonabil de asigurare că măsurile propuse sunt adecvate sau proporționale cu riscurile, având în vedere că riscurile respective nu au fost identificate inițial.

Grupul de lucru regretă profund că acest punct nu a fost abordat de către autorii cadrului propus.

Un cadru de evaluare a impactului asupra protecției datelor și a vieții private trebuie, prin definiție, să propună o metodologie generală în care faza de evaluare a riscurilor să reprezinte o componentă cheie. Cu siguranță, industria RFID realizează deja evaluări ale riscurilor în cadrul unei abordări metodologice în contextul gestionării securității informațiilor, conform definiției din ISO/IEC 27005[8] și din alte standarde naționale sau internaționale. Grupul de lucru este convins că industria RFID se poate baza pe această expertiză vastă din domeniul tradițional al gestionării securității informațiilor pentru a îmbogăți cadrul propus cu o abordare relevantă de evaluare a riscurilor. Acest lucru ar avea un impact și asupra altor elemente specifice din cadrul propus, așa cum se evidențiază mai ales în secțiunile 2.2, 2.3 și 2.4 din prezentul aviz.

În plus, considerentul 17 din recomandarea privind RFID precizează că elaborarea cadrului PIA *„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)”*. Acest fapt îndreptățește autorii cadrului propus să acorde o atenție deosebită avizului recent adoptat de către ENISA privind cadrul PIA[9] și să solicite orientări suplimentare din partea agenției UE cu privire la punerea în aplicare a abordării de evaluare a riscurilor în contextul RFID. ENISA și-a asumat în mod expres[10] *„sarcina de a identifica și evalua riscurile emergente și viitoare ale unui scenariu IoT/RFID specific, mai ales în contextul rolului ENISA în acest scenariu, prevăzut în Comunicarea CE „Internetul obiectelor – un plan de acțiune pentru Europa[11]”*. **Grupul de lucru încurajează puternic industria să profite de această ocazie.**

## 2.2 Etichete deținute de persoane

Unul dintre cele 3 motive principale de îngrijorare legate de respectarea vieții private evidențiate în *Documentul de lucru privind aspecte legate de protecția datelor conexe tehnologiei RFID (GL 105)*[12] *„este cauzat de utilizări ale tehnologiei RFID care permit urmărirea indivizilor și obținerea accesului la date cu caracter personal”*. Într-adevăr, elementele etichetate deținute de o persoană conțin identificatori

[8] A se vedea ISO/IEC 27001:2005, Tehnologia informației – Tehnici de securitate – Sisteme de gestionare a securității informațiilor – Cerințe

[9] Avizul ENISA privind o propunere din partea industriei pentru un cadru de evaluare a impactului asupra protecției datelor și a vieții private în cazul aplicațiilor RFID, iulie 2010, http://www.enisa.europa.eu/media/news-items/enisa-opinion-on-pia

[10] A se vedea, de exemplu, raportul ENISA intitulat „Zborurile 2.0 – Facilitarea călătoriilor aeriene automatizate prin identificarea și soluționarea provocărilor tehnologiei IoT & RFID”.

[11] Comisia Europeană, Comunicarea Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor: Internetul obiectelor – un plan de acțiune pentru Europa, COM(2009) 278, Bruxelles, 18. 6.2009

[12] A se vedea nota de subsol 2.

unici care ar putea fi citiți de la distanță. La rândul lor, acești identificatori unici ar putea fi utilizați pentru a recunoaște o anumită persoană de-a lungul timpului, aceasta devenind astfel „identificabilă". În unele cazuri, acest lucru poate fi de dorit, în special dacă un element etichetat este special creat pentru a fi utilizat ca mecanism de control al accesului (de exemplu: o cartelă de acces). Însă, în alte cazuri, apare posibilitatea ca o persoană să fie urmărită[13] fără știrea sa de către o parte terță. Așa cum se evidențiază în *Avizul nr. 4/2007 privind conceptul de date cu caracter personal* (GL 136)[14], atunci când un identificator unic este asociat cu o persoană, acesta se încadrează în definiția datelor cu caracter personal stabilită în Directiva 95/46/CE, indiferent de faptul că „identitatea socială" (numele, adresa etc.) a persoanei rămâne necunoscută (respectiv, ea este „identificabilă", însă nu neapărat „identificată").

În plus, numărul unic conținut într-o etichetă poate, de asemenea, reprezenta un mijloc de identificare de la distanță a naturii obiectelor deținute de o persoană, care, la rândul lor, pot dezvălui informații despre statutul social, starea de sănătate sau altele. Astfel, chiar și în acele cazuri în care o etichetă conține exclusiv un număr care este unic într-un anumit context și niciun alt fel de date cu caracter personal suplimentare, este necesară o atenție deosebită pentru a rezolva potențialele probleme legate de respectarea vieții private și securitate dacă eticheta va fi deținută de către persoane.

Grupul de lucru apreciază faptul că industria a recunoscut această problemă în cadrul PIA, solicitând o evaluare PIA atunci când *„etichetele cu nivelul elementului urmează să intre în posesia indivizilor"* (aplicații „de nivel 1").

Din păcate, în ciuda acestei premise, **cadrul propus** nu urmărește până la capăt acest motiv de îngrijorare și **nu invită în mod explicit operatorul RFID să evalueze problemele legate de respectarea vieții private și protecția datelor care ar putea apărea atunci când etichetele sunt deținute de către indivizi în viața de zi cu zi.** Nu este suficient să se stabilească *„dacă locația Indivizilor sau Utilizatorilor va fi monitorizată prin aplicația RFID[15]"*. Este, de asemenea, extrem de important să se analizeze riscul unei monitorizări neautorizate în afara perimetrului aplicației. Cadrul nu descrie nici măsurile luate pentru a elimina aceste riscuri. **Grupul de lucru îndeamnă industria să rezolve integral această problemă, menționând-o clar în cadru, ca parte componentă a unei abordări revizuite de evaluare a riscurilor.**

## *2.3 RFID în sectorul comerțului cu amănuntul*

Sectorul comerțului cu amănuntul este unul dintre domeniile de aplicare cheie în cadrul căruia etichetele ar putea ajunge să fie deținute de către indivizi. Recomandarea privind RFID a identificat acest sector drept unul critic și l-a abordat prin puncte specifice.

Punctul 11 din recomandarea privind RFID indică, în mod expres, următoarele: *„Comercianții cu amănuntul trebuie să dezactiveze sau să înlăture la punctul de vânzare etichetele utilizate în aplicația lor, cu excepția cazului în care consumatorii [...] acceptă ca etichetele să rămână operaționale"*.

Punctul 12 permite o excepție de la această regulă prevăzând că *„Punctul 11 nu ar trebui să se aplice atunci când din evaluarea impactului asupra protecției datelor și a vieții private reiese că etichetele care*

[13] A se vedea exemplele prezentate în GL 105, secțiunea 3.3.
[14] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf.
[15] La secțiunea 2.3.4 din cadrul propus.

*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".* Acest lucru înseamnă că dezactivarea la punctul de vânzare reprezintă comportamentul predefinit, cu excepția cazului în care PIA prevede altfel.

Cu toate acestea, secțiunea D din cadrul PIA propus oferă doar două concluzii posibile la un raport PIA: aplicația RFID fie *„este gata de implementare"*, fie *„nu este gata de implementare",* fără a oferi operatorului RFID posibilitatea de a formula o concluzie privind utilizarea etichetelor în afara punctului de vânzare la aplicațiile comercializate cu amănuntul, conform cerințelor din recomandarea privind RFID. Grupul de lucru constată că, în anumite scopuri, în sectorul comerțului cu amănuntul, unele aplicații pot justifica sau necesita ca mai multe etichete să rămână active în afara punctului de vânzare. Cu toate acestea, absența unei precizări de acest tip în cadrul propus pare să sugereze că toate etichetele vor fi dezactivate la punctul de vânzare.

Într-un sens mai larg, grupul de lucru observă că alegerea dual oferită în secțiunea D a cadrului PIA pare excesiv de restrictivă pentru operatorii RFID și pentru industria RFID în ansamblu. Unele aplicații pot fi considerate „gata de implementare în anumite condiții" care ar trebui descrise în concluziile raportului PIA.

**Grupul de lucru invită autorii cadrului propus să clarifice problema dezactivării etichetelor în sectorul comerțului cu amănuntul.** Cadrul propus trebuie să impună, în mod explicit, unui operator RFID să trateze punctul 12 din recomandarea privind RFID în raportul PIA care va fi întocmit (în cazul aplicațiilor din sectorul comerțului cu amănuntul). **În sens mai larg, o abordare revizuită de evaluare a riscurilor trebuie să ofere instrumentele adecvate pentru a se ajunge la o concluzie cu privire la condițiile de implementare ale unei aplicații RFID.**

## *2.4 Mențiuni suplimentare*

Așa cu s-a subliniat mai sus la secțiunea 2.2, dacă eticheta este deținută de către o persoană (fie aceasta un Utilizator sau Individ) și dacă eticheta conține un cod unic de identificare[16], atunci, prin definiție, eticheta conține date cu caracter personal. Strict vorbind, definițiile „aplicațiilor de nivel 1" și „aplicațiilor de nivel 0" prezentate la secțiunea 1.5 sunt, în consecință, contradictorii: în majoritatea scenariilor, nu este posibil să se afirme că aplicația RFID *nu* prelucrează date cu caracter personal dacă etichetele sunt deținute de către Indivizi sau Utilizatori. Prin urmare, conform acestor definiții, majoritatea aplicațiilor s-ar încadra în categoria aplicațiilor de nivel 2. **Astfel, aplicațiile de nivel 0 sau nivel 1 ar fi valabile doar în cazuri rare, în care etichetele sunt deținute de persoane și, totuși, nu includ un număr unic.**

Grupul de lucru pornește de la ideea că autorii cadrului nu au intenționat să stabilească un domeniu de aplicare atât de limitat pentru aplicațiile de nivel 0 și de nivel 1 și că definițiile acestora erau menite să cuprindă aplicațiile care prelucrează doar un singur tip de date cu caracter personal, respectiv, codul unic de identificare al etichetei. Toate definițiile nivelurilor ar putea fi clarificate cu ușurință pentru a elimina orice ambiguitate. În orice caz, definirea adecvată a unei metodologii bazate pe evaluarea riscurilor ar putea determina, de asemenea, o reformulare a acestor definiții.

[16] Ne referim, în sens mai larg, la „codul unic de identificare al etichetei" pentru a desemna orice număr unic de identificare (sau număr de serie) care poate fi accesat pe eticheta RFID și care permite caracterizarea unică a unei etichete RFID într-un anumit context.

Grupul de lucru constată că în cadru se face referire la etichetele *„aflate în posesia”* Utilizatorilor sau Indivizilor. Această formulare este prea restrictivă și ar trebui înlocuită cu „deținute”, cuvânt care descrie mult mai corect scenariile de risc existente.

Grupul de lucru este de părere că procesul PIA propus în cadru trebuie să includă o fază de consultare a părților interesate. Aceasta presupune consultarea părților interesate (grupuri, sindicate, asociații…) care pot fi afectate de aplicația RFID, precum și schimbul de idei, sugestii și metode de îmbunătățire care vor permite implementarea aplicației într-o manieră deschisă și cu respectarea vieții private, ceea ce va aduce beneficii atât operatorului RFID, cât și Utilizatorilor sau Indivizilor afectați. O astfel de fază de consultare a părților interesate contribuie în mod clar la *„informațiile și la transparența privind utilizarea RFID”*, precum și la *„acțiunile de sensibilizare”* prevăzute de recomandarea privind RFID.

De asemenea, grupul de lucru subliniază că, pentru a fi prelucrate în mod legal și în condiții de siguranță, categoriile speciale de date[17] necesită condiții specifice. Cadrul ar trebui să ofere operatorului RFID orientări mai clare privind problemele specifice legate de prelucrarea categoriilor speciale de date. De asemenea, identificarea utilizării categoriilor speciale de date ar trebui să facă parte din orice proces de evaluare a riscurilor.

Cadrul ar trebui să ofere, de asemenea, operatorilor RFID orientări privind cele mai adecvate termene și condiții pentru realizarea unei evaluări PIA în cursul ciclului de dezvoltare al unui produs RFID, pentru a încuraja în mod real *„securitatea și respectarea vieții private din momentul proiectării”,* astfel cum susține recomandarea.

# 3 Concluzie

Din cauza problemelor evidențiate în prezentul aviz, în special din cauza absenței din cadrul propus a unei abordări clare și cuprinzătoare de evaluare a riscurilor pentru protecția datelor și a vieții private, **grupul de lucru nu aprobă documentul propus în forma sa actuală.**

Este necesar să se sublinieze că includerea unui proces adecvat de evaluare a riscurilor poate facilita în mod clar rezolvarea marii majorități a celorlalte probleme identificate în prezentul aviz. Într-adevăr, dacă unui operator RFID i se solicită să realizeze o evaluare a riscurilor, acesta va identifica mai ales riscurile asociate cu monitorizarea neautorizată a etichetelor RFID deținute de persoane. În plus, în sectorul comerțului cu amănuntul, ar putea fi utilă prezentarea unui caz clar care să ilustreze că anumite etichete RFID (utilizate într-o aplicație specifică) care *„rămân operaționale dincolo de punctul de vânzare nu prezintă un risc potențial la adresa protecției datelor personale sau a vieții private”*.

[17] Articolul 8 din Directiva 95/46/CE.

Grupul de lucru își exprimă convingerea că industria poate propune un cadru îmbunătățit pe baza observațiilor care au fost evidențiate în prezentul aviz și își asumă angajamentul de a urmări toate căile relevante pentru a îmbunătăți și mai mult cadrul propus și pentru a urgenta aprobarea acestuia.

Adoptat la Bruxelles, la 13 iulie 2010

*Pentru grupul de lucru*
*Președintele*
*Jacob KOHNSTAMM*