ПРЕПОРЪКИ

КОМИСИЯ

ПРЕПОРЪКА НА КОМИСИЯТА

от 12 май 2009 година

относно спазването на принципите за неприкосновеност на личния живот и защита на данните в приложения, използващи радиочестотна идентификация

(нотифицирано под номер C(2009) 3200)

(2009/387/ЕО)

КОМИСИЯТА НА ЕВРОПЕЙСКИТЕ ОБЩНОСТИ,

като взе предвид Договора за създаване на Европейската общност, и по-специално член 211 от него,

след консултация с Европейския надзорен орган по защита на данните,

като има предвид, че:

(1) Радиочестотната идентификация (RFID) представлява ново развитие в информационното общество, при което обекти, снабдени с микроелектронни елементи, способни да обработват информация самостоятелно, ще навлизат все повече в ежедневния живот.

(2) RFID се превръща все повече в обичайна технология и по този начин в част от живота на отделните индивиди в множество области като например логистиката [1], здравеопазването, обществения транспорт, търговията на дребно, по-специално за подобряване на сигурността на продуктите и по-бързо изтегляне на продукти от употреба, развлеченията, работата, събирането на такси по пътищата, управлението на доставки на багаж и пътните документи.

(3) В икономическо отношение технологията RFID е многообещаваща и може да създаде нови възможности за бизнес, за намаляване на разходите и повишаване на ефективността, по-специално за овладяване на проблематиката с фалшификатите и за управление на електронните отпадъци, опасните материали, за рециклиране на продукти в края на техния жизнен цикъл, като по този начин притежава потенциал да се превърне в нов двигател на растежа и създаването на работни места и така да даде значителен принос за постигане на целите на Лисабонската стратегия.

(4) Технологията RFID позволява предаването на къси разстояния на данни, в това число и на лични данни, без физически контакт или видимо взаимодействие между четящото или записващото устройство и етикета, така че взаимодействието може да се осъществи без съответният индивид да забележи това.

(5) RFID приложенията са в състояние да обработват данни, свързани с вече идентифицирано или подлежащо на идентифициране физическо лице, като идентифицирането на физическото лице може да бъде пряко или косвено. Те могат да обработват лични данни, записани в етикета, като име, рождена дата, адрес на лицето, биометрични данни или специален номер на RFID елемента, позволяващ свързването на последния с лични данни, съхранявани в други части на системата. Освен това тази технология може да се използва за проследяване на индивиди по номерата на притежаваните от тях един или повече обекти, снабдени с RFID елементи.

(6) Поради потенциала на тази технология да бъде както повсеместна, така и практически невидима, особено внимание при разпространяването на RFID следва да се обърне на въпросите на неприкосновеността на личния живот и защитата на данните. Следователно преди пускането им в широка употреба, RFID приложенията следва да бъдат пригодени към изискванията за неприкосновеност на личния живот и информационна сигурност (принцип на „гарантиране на сигурността и неприкосновеността на личния живот чрез конструктивното решение“).

(7) Многобройните икономически и обществени ползи от RFID ще могат да се реализират, само ако съществуват ефективни мерки за гарантиране на сигурността на данните, неприкосновеността на личния живот и свързаните с тях етични принципи, които са в основата на дебата за общественото приемане на RFID.

(8) Държавите-членки и заинтересованите страни следва да положат допълнителни усилия, особено на настоящия начален етап на разпространение на радиочестотната идентификация, за да гарантират надзора на RFID приложенията и спазването на правата и свободите на индивидите.

[1] COM(2007) 607 окончателен.

(9) В съобщението на Комисията от 15 март 2007 г. „Радиочестотната идентификация (RFID) в Европа: стъпки към изграждане на политическа рамка“ ([1]) се посочва, че под формата на една или повече препоръки на Комисията ще бъдат предоставени пояснения и насоки във връзка с аспектите на защитата на данните и неприкосновеността на личния живот при RFID приложенията.

(10) Правата и задълженията относно опазването на личните данни и свободното движение на тези данни, както са определени с Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 година за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни ([2]) и с Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 година относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронни комуникации) ([3]), важат напълно при използването на RFID приложения, обработващи лични данни.

(11) Принципите, определени от Директива 1999/5/ЕО на Европейския парламент и на Съвета от 9 март 1999 г. относно радионавигационното оборудване и далекосъобщителното крайно оборудване и взаимното признаване на тяхното съответствие ([4]), следва да бъдат прилагани към разработването на RFID приложения.

(12) В своето становище Европейският надзорен орган по защита на данните ([5]) дава насоки за работа с продукти, снабдени с етикети и предназначени за индивидуална употреба, и изисква да бъдат направени оценки на въздействието върху неприкосновеността на личния живот и сигурността, за да бъдат открити и разработени „най-добрите достъпни технологии“ за гарантиране на неприкосновеността на личния живот и сигурността при системи с RFID.

(13) Операторите на RFID приложения следва да предприемат всички уместни стъпки, за да гарантират, че не е възможно данните да бъдат свързани с определено идентифицирано или подлежащо на идентифициране физическо лице с някое от средствата, използвани евентуално от оператора на RFID приложения или от кое да е друго лице, освен в случаите, когато такива данни се обработват съгласно приложимите принципи и законови норми за защита на данни.

(14) В съобщението на Комисията от 2 май 2007 г. относно насърчаване на защитата на личните данни чрез технологиите за подобряване на защитата на личния живот (PETs) ([6]) се определят ясно действията, необходими за постигане на целта за минимизиране на обработката на лични данни и използване на анонимни и псевдоанонимни данни, когато това е възможно, чрез подпомагане на разработката на PETs и тяхното използване от контролни органи и индивиди.

(15) В съобщението на Комисията от 31 май 2006 г. „Стратегия за сигурност на информационното общество — Диалог, партньорство и правомощия“ ([7]) се потвърждава, че многообразието, отвореността, оперативната съвместимост, приложимостта и конкуренцията са основни фактори за постигане на сигурно информационно общество, посочва се ролята на държавите-членки и публичните администрации за повишаване на осведомеността и насърчаване на добрите практики относно сигурността, и се приканват заинтересованите страни от частния сектор да поемат инициативата при разработването на системи за сигурност с икономически приемливи схеми за удостоверяване на продукти, процеси и услуги, които са насочени към специфичните нужди на ЕС, по-специално по отношение на неприкосновеността на личния живот.

(16) С Резолюция на Съвета от 22 март 2007 г. относно Стратегия за сигурност на информационното общество в Европа ([8]) държавите-членки се приканват да отделят необходимото внимание на нуждата от предотвратяване на и борбата с нови и съществуващи заплахи за сигурността на електронните съобщителни мрежи.

(17) Съгласуваното прилагане на разпоредбите на настоящата препоръка от държавите-членки ще бъде гарантирано от една разработена на равнището на Общността рамка за провеждане на оценки на въздействието върху неприкосновеността на личния живот и защитата на данните. Тази рамка следва да бъде разработена на базата на наличните практики и опит, събран в държавите-членки, в трети държави и при работата на Европейската агенция за мрежова и информационна сигурност (ENISA) ([9]).

(18) Комисията ще осигури разработването на насоки относно управлението на информационната сигурност на RFID приложения на ниво Общност, като се основава на съществуващи практики и опит, събран в държавите-членки и в трети държави. Държавите-членки следва да се включат в този процес и да насърчат участието на частни и публични институции.

(19) Необходимата за вземането на подходящи предохранителни мерки информация ще бъде осигурена чрез оценка на въздействието върху неприкосновеността на личния живот и защитата на данните, провеждана от оператора преди създаването на дадено RFID приложение. Тези мерки ще трябва да бъдат следени и преразглеждани в рамките на жизнения цикъл на RFID приложението.

(20) В областта на търговията на дребно необходимата информация за установяване на потенциални заплахи за неприкосновеността на личния живот или защитата на лични данни ще бъде набавена чрез оценка на въздействието на продукти, снабдени с етикети и предназначени за индивидуална употреба, върху неприкосновеността на личния живот или защитата на данни.

([1]) COM(2007) 96 окончателен.
([2]) ОВ L 281, 23.11.1995 г., стр. 31.
([3]) ОВ L 201, 31.7.2002 г., стр. 37.
([4]) ОВ L 91, 7.4.1999 г., стр. 10.
([5]) ОВ C 101, 23.4.2008 г., стр. 1.
([6]) COM(2007) 228 окончателен.
([7]) COM(2006) 251 окончателен.
([8]) ОВ C 68, 24.3.2007 г., стр. 1.
([9]) Член 2, параграф 1 от Регламент (ЕО) № 460/2004 на Европейския парламент и на Съвета (ОВ L 77, 13.3.2004 г., стр. 1).

(21) Прилагането на международни стандарти като тези, разработени от Международната организация по стандартизация (ISO), на кодекси за поведение и на най-добри практики, съобразени с регулаторната рамка на ЕС, може да подпомогне управлението на информационната сигурност и мерките относно неприкосновеността на личния живот във всяка фаза на базираните на RFID търговски процеси.

(22) Необходими са подходящи защитни мерки във връзка с RFID приложения, засягащи широката публика, от рода на електронните билети в обществения транспорт. RFID приложения, засягащи индивиди чрез обработката например на биометрични данни за самоличност или на данни за здравословното състояние, са особено критични по отношение на информационната сигурност и неприкосновеността на личния живот и поради тази причина изискват специално внимание.

(23) Обществото като цяло трябва да е наясно със задълженията и правата, които възникват при употребата на RFID приложения. Поради тази причина страните, разпространяващи технологията, поемат задължение да информират индивидите относно употребата на тези приложения.

(24) Повишаването на осведомеността на публиката и на малките и средни предприятия (МСП) относно характеристиките и възможностите на технологията RFID ще допринесе за постигането на очакваните икономически резултати и същевременно ще намали рисковете от използването ѝ в ущърб на обществените интереси, като по този начин ще увеличи нейната приемливост.

(25) Комисията ще даде своя принос към прилагането на настоящата препоръка по пряк и косвен начин, като улесни диалога и сътрудничеството между заинтересованите страни, по-специално чрез Рамковата програма за конкурентоспособност и иновации (РПКИ), създадена с Решение № 1639/2006/ЕО на Европейския парламент и на Съвета ([1]), и Седмата рамкова програма за научни изследвания (РП7), създадена с Решение № 1982/2006/ЕО на Европейския парламент и на Съвета ([2]).

(26) Проучването и разработката на евтини технологии за защита на неприкосновеността на личния живот и за информационна сигурност е от съществено значение за насърчаването на нивото на Общността на по-широкото разпространение на тези технологии при приемливи условия.

(27) Настоящата препоръка спазва основните права и зачита принципите, признати по-специално в Хартата на основните права на Европейския съюз. Настоящата препоръка се стреми да гарантира по-специално пълното зачитане на личния и семейния живот и защитата на личните данни,

([1]) ОВ L 310, 9.11.2006 г., стр. 15.
([2]) ОВ L 412, 30.12.2006 г., стр. 1.

ПРЕПОРЪЧВА:

Приложно поле

1. Настоящата препоръка предлага насоки за държавите-членки относно проектирането и използването на RFID приложения по законосъобразен, етичен и приемлив от социална и политическа гледна точка начин, като зачита правото на неприкосновеност на личния живот и осигурява защитата на личните данни.

2. Настоящата препоръка предлага насоки относно мерките, които трябва да бъдат взети при разпространението на RFID приложения, така че да се гарантира, когато е необходимо, спазването на националното законодателство за прилагане на директиви 95/46/ЕО, 1999/5/ЕО и 2002/58/ЕО.

Определения

3. За целите на използването на настоящата препоръка следва да се прилагат определенията, посочени в Директива 95/46/ЕО. Следва да се прилагат също следните определения:

а) „радиочестотна идентификация“ (RFID) означава използването на електромагнитни вълни или индуктивна връзка в радиочестотната част на спектъра за осъществяване на връзка към или от етикет с помощта на различни методи за модулация и кодиране с цел прочитане на идентификационния знак на радиочестотен етикет или на други съхранявани в него данни;

б) „RFID етикет“ или „етикет“ означава RFID устройство, способно да произвежда радиосигнал, или RFID устройство, което модулира и връща, излъчва обратно или отразява (в зависимост от вида на устройството) получен от четящо или записващо устройство сигнал с носеща честота;

в) „RFID четящо или записващо устройство“ или „четец“ означава стационарно или мобилно устройство за събиране на данни и идентификация, което използва електромагнитни вълни в радиочестотния спектър или електромагнитна индукция, за да породи и предизвика в отговор излъчването на модулирани данни от етикет или група етикети;

г) „RFID приложение“ или „приложение“ означава приложение, което обработва данни с помощта на поддържаща система и на мрежова инфраструктура, като използва етикети и четящи устройства;

д) „оператор на RFID приложение“ или „оператор“ означава физическо или юридическо лице, обществен орган, агенция или коя да е друга институция, която самостоятелно или съвместно с други определя целите и начините на използване на дадено приложение, в това число и контролните органи по защитата на личните данни при експлоатацията на дадено RFID приложение;

е) „информационна сигурност“ означава запазването на поверителността, целостта и достъпността на информацията;

ж) „проследяване“ означава всяка дейност, насочена към откриване, наблюдаване, копиране или записване на данни за местоположението, движението, действията или състоянието на даден индивид.

Оценки на въздействието върху неприкосновеността на личния живот и защитата на данните

4. Държавите-членки следва да вземат мерки за разработването от страна на промишлеността, в сътрудничество със съответни заинтересовани страни, представящи гражданското общество, на рамка за провеждане на оценки на въздействието върху неприкосновеността на личния живот и защитата на данните. Тази рамка следва да бъде представена на Работната група за защита на личните данни по член 29 в срок от 12 месеца след публикуването на настоящата препоръка в *Официален вестник на Европейския съюз*.

5. Държавите-членки следва да гарантират, че операторите, без да се засягат техните задължения съгласно Директива 95/46/ЕО:

а) извършват оценка на въздействието на приложението върху неприкосновеността на личния живот и защитата на данните, в това число и дали приложението може да бъде използвано за проследяване на индивиди. Степента на подробност на оценката следва да отговаря на рисковете за неприкосновеността на личния живот, свързани с приложението;

б) вземат подходящи технически и организационни мерки, за да гарантират защитата на личните данни и на неприкосновеността на личния живот;

в) избират лице или група от лица, отговарящи за преразглеждане на оценките и на пригодността на техническите и организационните мерки за гарантиране на защитата на личните данни и на неприкосновеността на личния живот;

г) осигуряват достъп на компетентния орган до резултатите от оценката не по-късно от шест седмици преди пускането в действие на приложението;

д) изпълняват предходните разпоредби веднага след като определената в точка 4 рамка за провеждане на оценки на въздействието върху неприкосновеността на личния живот и защитата на данните стане достъпна.

Информационна сигурност

6. Държавите-членки следва да подкрепят Комисията при определяне на приложенията, които могат да породят заплахи за информационната сигурност по отношение на широката публика. За такъв вид приложения държавите-членки следва да гарантират, че операторите, съвместно с компетентните органи и организации на гражданското общество, ще разработят нови или ще приложат вече съществуващи схеми от рода на сертифицирането или самооценката на оператори, за да демонстрират постигането на подходящо ниво на информационна сигурност и неприкосновеност на личния живот по отношение на оценените рискове.

Информация и прозрачност относно употребата на RFID

7. Без да се засягат задълженията на контролните органи за данни съгласно директиви 95/46/ЕО и 2002/58/ЕО, държавите-членки следва да гарантират, че операторите ще разработят и публикуват подробна, точна и лесна за разбиране информационна политика за всяко от своите приложения. Политиката следва да включва поне:

а) самоличност и адрес на оператора;

б) предназначение на приложението;

в) какви данни се обработват от приложението, особено ако се обработват лични данни, и дали се проследява местоположението на етикетите;

г) обобщение на оценката на въздействието върху неприкосновеността на личния живот и защитата на данните;

д) очакваните рискове, ако има такива, за неприкосновеността на личния живот, свързани с използването на етикети от приложението и мерките, които могат да вземат индивидите за намаляване на тези рискове.

8. Държавите-членки следва да гарантират, че операторите ще предприемат стъпки за информиране на индивидите за наличието на четящи устройства посредством общоевропейски знак, разработен от европейските организации по стандартизация с подкрепата на заинтересованите страни. Знакът трябва да дава информация за самоличността на оператора и за пункта за контакти, където индивидът може да се осведоми за информационната политика на приложението.

RFID приложения в търговията на дребно

9. Посредством общоевропейския знак, разработен от европейските организации по стандартизация с подкрепата на заинтересованите страни, операторите следва да информират индивидите за наличието на етикети, прикрепени към или вградени в продуктите.

10. При извършването на оценката на въздействието върху неприкосновеността на личния живот и защитата на данните, както е посочено в точки 4 и 5, операторът на дадено приложение следва изрично да установи дали етикети, прикрепени към или вградени в продукти, продавани на потребители от търговци, които не са оператори на даденото приложение, представляват евентуална заплаха за неприкосновеността на личния живот или защитата на данни.

11. Търговците на дребно следва да деактивират или да отстранят в момента на продажбата етикетите, използвани от тяхното приложение, освен ако потребителите, след като са били информирани за политиката, посочена в точка 7, изразят своето съгласие етикетите да останат активни. Под деактивиране на етикетите се разбира процесът, който спира онези взаимодействия на етикета с неговото обкръжение, които не изискват активното участие на потребителя. Деактивирането или отстраняването на етикетите от търговеца следва да бъде извършено незабавно и безвъзмездно за потребителя. Потребителите трябва да могат да се уверят, че деактивирането или отстраняването са били ефективни.

12. Точка 11 не следва да се прилага, ако оценката на въздействието върху неприкосновеността на личния живот и защитата на данните констатира, че ако използваните в дадено търговско приложение етикети останат активни след напускането на точката на продажба, това не би представлявало заплаха за неприкосновеността на личния живот и защитата на данните. Независимо от това търговците следва да осигурят достъп до лесни и безплатни средства за незабавно или по-късно деактивиране или отстраняване на тези етикети.

13. Деактивирането или отстраняването на етикети не следва да води до намаляване или прекратяване на законните задължения на търговеца или производителя спрямо потребителя.

14. Точки 11 и 12 следва да се прилагат само към търговци, които са оператори.

Дейности за повишаване на осведомеността

15. Държавите-членки, в сътрудничество с промишлеността, Комисията и други заинтересовани страни, следва да предприемат подходящи мерки за информиране и повишаване на осведомеността на публичните органи и предприятията, особено на МСП, относно потенциалните ползи и рискове, свързани с използването на технологията RFID. Особено внимание следва да бъде отделено на информационната сигурност и неприкосновеността на личния живот.

16. Държавите-членки, в сътрудничество с промишлеността, асоциациите на гражданското общество, Комисията и съответните заинтересовани страни, следва да установят и предоставят примери за добри практики при употребата на RFID приложения за информиране и повишаване на осведомеността сред широката публика. Освен това те следва да предприемат подходящи мерки като например широкомащабни пилотни проекти за повишаване на осведомеността относно технологията RFID, и относно ползите, рисковете и последствията от използването ѝ, като предпоставка за широкото разпространение на тази технология.

Научноизследователска и развойна дейност

17. Държавите-членки следва да си сътрудничат с промишлеността, съответните заинтересовани страни на гражданското общество и Комисията, за да насърчат и подкрепят въвеждането на принципа на „гарантиране на сигурността и неприкосновеността на личния живот чрез конструктивното решение“ в началния етап на разработката на RFID приложения.

Последващи действия

18. Държавите-членки следва да предприемат всички необходими мерки, за да предоставят настоящата препоръка на вниманието на всички заинтересовани страни, които участват в проектирането и експлоатацията на RFID приложения в Общността.

19. Държавите-членки следва да информират Комисията в срок от 24 месеца след публикуването на настоящата препоръка в *Официален вестник на Европейския съюз* за действията, предприети в отговор на настоящата препоръка.

20. В срок от три години след публикуването на настоящата препоръка в *Официален вестник на Европейския съюз* Комисията ще представи доклад за прилагането на тази препоръка, нейната ефективност и нейното въздействие върху операторите и потребителите, по-специално по отношение на мерките, препоръчани в точки 9—14.

Адресати

21. Адресати на настоящата препоръка са държавите-членки.

Съставено в Брюксел на 12 май 2009 година.

За Комисията

Viviane REDING

Член на Комисията