ZALECENIA

KOMISJA

ZALECENIE KOMISJI

z dnia 12 maja 2009 r.

w sprawie wdrażania zasad ochrony prywatności i ochrony danych w zastosowaniach wspieranych identyfikacją radiową

(notyfikowana jako dokument nr C(2009) 3200)

(2009/387/WE)

KOMISJA WSPÓLNOT EUROPEJSKICH,

uwzględniając Traktat ustanawiający Wspólnotę Europejską, w szczególności jego art. 211,

po zasięgnięciu opinii Europejskiego Inspektora Ochrony Danych,

a także mając na uwadze, co następuje:

(1) Identyfikacja radiowa (RFID) stanowi nowy etap rozwoju społeczeństwa informacyjnego, w którym obiekty wyposażone w mikroelektronikę, mogącą automatycznie przetwarzać dane, w coraz większym stopniu będą stawały się integralną częścią życia codziennego.

(2) Stopniowo zwiększa się powszechność identyfikacji radiowej, która tym samym staje się częścią życia osób fizycznych w wielu różnych dziedzinach, takich jak: logistyka ([1]), opieka zdrowotna, transport publiczny, handel detaliczny, w szczególności w zakresie poprawy bezpieczeństwa produktów i szybszego wycofywania produktów z rynku, rozrywka, praca, zarządzanie opłatami drogowymi, zarządzanie bagażem i dokumenty podróży.

(3) Technologia RFID może stać się nowym motorem wzrostu gospodarczego i zatrudnienia, a tym samym stanowić znaczący wkład w realizację strategii lizbońskiej, ponieważ jest bardzo obiecująca z ekonomicznego punktu widzenia – może pociągać za sobą nowe możliwości działalności gospodarczej, obniżenie kosztów i wzrost wydajności, w szczególności w zakresie radzenia sobie z podrabianiem produktów, zarządzania odpadami elektronicznymi i materiałami niebezpiecznymi, a także recyklingu zużytych produktów.

(4) Technologia identyfikacji radiowej umożliwia przetwarzanie danych, w tym danych osobowych, na niewielkich odległościach bez fizycznego lub widocznego kontaktu między czytnikiem lub urządzeniem zapisującym a identyfikatorem, w ten sposób, że dana osoba nie ma świadomości tego kontaktu.

(5) Zastosowania technologii RFID mają możliwość przetwarzania danych dotyczących zidentyfikowanej lub identyfikowalnej osoby fizycznej, przy czym osoba fizyczna jest identyfikowana bezpośrednio lub pośrednio. Mogą również przetwarzać takie dane osobowe przechowywane w identyfikatorze jak nazwisko osoby, data urodzenia, adres, dane biometryczne lub dane łączące poszczególny numer RFID produktu z danymi osobowymi przechowywanymi w innym miejscu w systemie. Ponadto istnieje możliwość wykorzystywania tej technologii do monitorowania osób fizycznych na podstawie posiadania przez nie jednego lub więcej produktów zawierających numer RFID produktu.

(6) Przy wdrażaniu technologii RFID należy zwrócić szczególną uwagę na prywatność i ochronę danych, gdyż rozwiązania te mogą być jednocześnie wszechobecne i praktycznie niewidoczne. W związku z tym elementy prywatności i bezpieczeństwa informacji należy włączyć do zastosowań identyfikacji radiowej przed ich powszechnym wykorzystaniem (zasada „bezpieczeństwa i poszanowania prywatności od samego początku").

(7) Technologia RFID będzie mogła przynosić liczne korzyści gospodarcze i społeczne tylko wtedy, gdy zostaną wprowadzone skuteczne środki w celu zapewnienia ochrony danych osobowych, prywatności i związanych z nimi zasad etycznych, które są centralnym punktem dyskusji na temat społecznej akceptacji technologii RFID.

(8) Państwa członkowskie i zainteresowane strony powinny dołożyć dalszych starań, aby, szczególnie w obecnej początkowej fazie wdrażania technologii RFID, zapewnić monitorowanie zastosowań technologii RFID i przestrzeganie praw i wolności jednostki.

([1]) COM(2007) 607 wersja ostateczna.

(9) W komunikacie Komisji z dnia 15 marca 2007 r. „Identyfikacja radiowa (RFID) w Europie: w stronę ram polityki" [1] zapowiedziano przedstawienie wyjaśnień i wytycznych dotyczących aspektów ochrony danych i prywatności zastosowań RFID w drodze jednego lub kilku zaleceń Komisji.

(10) Prawa i obowiązki dotyczące ochrony danych osobowych i ich swobodnego przepływu, określone w dyrektywie 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych [2] i w dyrektywie 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) [3], mają w pełni zastosowanie do wykorzystywania zastosowań RFID, które przetwarzają dane osobowe.

(11) Zasady określone w dyrektywie 1999/5/WE Parlamentu Europejskiego i Rady z dnia 9 marca 1999 r. w sprawie urządzeń radiowych i końcowych urządzeń telekomunikacyjnych oraz wzajemnego uznawania ich zgodności [4] należy stosować przy opracowaniu zastosowań RFID.

(12) Opinia Europejskiego Inspektora Ochrony Danych [5] zawiera wytyczne dotyczące sposobów postępowania z produktami zawierającymi identyfikatory dostarczanymi osobom fizycznym i wzywa do sporządzenia ocen skutków w zakresie prywatności i bezpieczeństwa celem określenia i opracowania „najlepszej dostępnej technologii", która zapewni ochronę prywatności i bezpieczeństwa systemów RFID.

(13) Operatorzy zastosowań RFID powinni podjąć wszelkie racjonalne działania mające na celu dopilnowanie, aby dane nie były – za pomocą jakiegokolwiek środka możliwego do użycia przez operatora rozwiązań RFID lub jakąkolwiek inną osobę – powiązane ze zidentyfikowaną lub identyfikowalną osobą fizyczną, chyba że dane te są przetwarzane zgodnie z mającymi zastosowanie zasadami i przepisami prawa dotyczącymi ochrony danych.

(14) Komunikat Komisji z dnia 2 maja 2007 r. w sprawie lepszej ochrony danych z wykorzystaniem technologii na rzecz ochrony prywatności [6] jasno określa działania prowadzące do ograniczenia przetwarzania danych osobowych i jak najpowszechniejszego wykorzystywania danych anonimowych lub pseudoanonimowych przez wspieranie rozwoju technologii na rzecz ochrony prywatności i wykorzystanie ich przez administratorów danych oraz użytkowników.

(15) Komunikat Komisji z dnia 31 maja 2006 r. „Strategia na rzecz bezpiecznego społeczeństwa informacyjnego – »Dialog, partnerstwo i przejmowanie inicjatywy«" [7] potwierdza, że różnorodność, otwartość, interoperacyjność, użyteczność i konkurencja są kluczowymi czynnikami dla bezpieczeństwa społeczeństwa informacyjnego, podkreśla rolę państw członkowskich i administracji publicznej w podnoszeniu świadomości i wspieraniu dobrych praktyk w dziedzinie bezpieczeństwa oraz zachęca zainteresowane strony z sektora prywatnego do podejmowania inicjatyw związanych z pracami na rzecz stworzenia przystępnych cenowo systemów certyfikacji bezpieczeństwa produktów, procesów i usług, dopasowanych do konkretnych potrzeb UE (w szczególności w odniesieniu do prywatności).

(16) Celem rezolucji Rady z dnia 22 marca 2007 r. w sprawie strategii na rzecz bezpiecznego społeczeństwa informacyjnego w Europie [8] jest zachęcenie państw członkowskich do zwrócenia należnej uwagi na potrzebę zapobiegania nowym i istniejącym zagrożeniom dla sieci łączności elektronicznej i zwalczania takich zagrożeń.

(17) Ramy opracowane na poziomie wspólnotowym w celu przeprowadzenia ocen skutków w zakresie ochrony danych i prywatności zapewnią spójne stosowanie się do przepisów niniejszego zalecenia we wszystkich państwach członkowskich. Opracowanie tych ram powinno opierać się na istniejących praktykach i doświadczeniach zdobytych w państwach członkowskich, w krajach trzecich i w ramach prac prowadzonych przez Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji (ENISA) [9].

(18) Komisja zapewni opracowanie na poziomie wspólnotowym wytycznych dotyczących zarządzania bezpieczeństwem informacji w zastosowaniach RFID, opierając się na istniejących praktykach i doświadczeniach zdobytych w państwach członkowskich i krajach trzecich. Państwa członkowskie powinny włączyć się w ten proces i zachęcać do uczestnictwa w nim również podmioty prywatne i władze publiczne.

(19) Ocena skutków w zakresie ochrony danych i prywatności przeprowadzona przez operatora przed wdrożeniem zastosowania RFID dostarczy informacji wymaganych do zapewnienia odpowiednich środków ochronnych. Potrzebne będzie monitorowanie i poddawanie przeglądowi tych środków w trakcie użytkowania zastosowania RFID.

(20) Ocena skutków w zakresie ochrony danych i prywatności w sektorze handlu detalicznego w odniesieniu do sprzedawanych klientom produktów zawierających identyfikatory dostarczy informacji koniecznych do określenia prawdopodobieństwa zagrożenia dla prywatności lub ochrony danych osobowych.

[1] COM(2007) 96 wersja ostateczna.
[2] Dz.U. L 281 z 23.11.1995, s. 31.
[3] Dz.U. L 201 z 31.7.2002, s. 37.
[4] Dz.U. L 91 z 7.4.1999, s. 10.
[5] Dz.U. C 101 z 23.4.2008, s. 1.
[6] COM(2007) 228 wersja ostateczna
[7] COM(2006) 251 wersja ostateczna
[8] Dz.U. C 68 z 24.3.2007, s. 1.
[9] Artykuł 2 ust. 1 rozporządzenia (WE) nr 460/2004 Parlamentu Europejskiego i Rady (Dz.U. L 77 z 13.3.2004, s. 1).

(21) Wykorzystanie międzynarodowych norm, takich jak normy opracowane przez Międzynarodową Organizację Normalizacyjną (ISO), kodeksów postępowania i najlepszych praktyk, zgodnych z ramami prawnymi UE, może pomóc w zarządzaniu bezpieczeństwem informacji i środkami ochrony prywatności podczas całego procesu biznesowego wykorzystującego identyfikację radiową.

(22) Zastosowania RFID mające skutki dla ogółu społeczeństwa, takie jak bilety elektroniczne w transporcie publicznym, wymagają odpowiednich środków ochronnych. Zastosowania RFID mające wpływ na osoby fizyczne poprzez przetwarzanie na przykład ich danych identyfikacji biometrycznej lub danych dotyczących zdrowia są szczególnie krytyczne w odniesieniu do bezpieczeństwa informacji i prywatności, w związku z czym wymagają szczególnej uwagi.

(23) Społeczeństwo jako całość musi mieć świadomość obowiązków i praw mających zastosowanie w związku z wykorzystywaniem rozwiązań RFID. Dlatego na stronach wdrażających tę technologię spoczywa odpowiedzialność dostarczenia osobom fizycznym informacji na temat wykorzystania tych zastosowań.

(24) Podnoszenie świadomości wśród społeczeństwa oraz małych i średnich przedsiębiorstw (MŚP) na temat cech i możliwości identyfikacji radiowej umożliwi tej technologii spełnienie oczekiwań gospodarczych i zmniejszy tym samym ryzyko wykorzystania jej ze szkodą dla interesu publicznego, podnosząc w ten sposób poziom jej akceptacji.

(25) Komisja będzie miała bezpośredni i pośredni wkład we wdrażanie niniejszego zalecenia przez ułatwienie dialogu i współpracy między zainteresowanymi stronami, w szczególności przy pomocy programu ramowego na rzecz konkurencyjności i innowacji (CIP), ustanowionego na mocy decyzji nr 1639/2006/WE Parlamentu Europejskiego i Rady [1], oraz siódmego programu ramowego w dziedzinie badań (FP7), ustanowionego na mocy decyzji nr 1982/2006/WE Parlamentu Europejskiego i Rady [2].

(26) Na poziomie wspólnotowym zasadnicze jest podjęcie prac badawczo-rozwojowych w odniesieniu do tanich technologii poprawy prywatności i bezpieczeństwa informacji w celu wspierania szerszego wykorzystania tych technologii zgodnie z dopuszczalnymi warunkami.

(27) Niniejsze zalecenie opiera się na poszanowaniu praw podstawowych i przestrzeganiu zasad uznanych w szczególności w Karcie praw podstawowych Unii Europejskiej. Celem niniejszego zalecenia jest w szczególności zapewnienie pełnego poszanowania życia prywatnego i rodzinnego oraz ochrony danych osobowych,

[1] Dz.U. L 310 z 9.11.2006, s. 15.
[2] Dz.U. L 412 z 30.12.2006, s. 1.

NINIEJSZYM ZALECA:

Zakres

1. Niniejsze zalecenie udziela wytycznych dla państw członkowskich w zakresie projektowania i działania zastosowań RFID w sposób dopuszczalny z punktu widzenia prawa, etyki oraz zasad społecznych i politycznych, z poszanowaniem prawa do prywatności i zapewnieniem ochrony danych osobowych.

2. Zalecenie to udziela również wytycznych dotyczących środków, które należy podjąć w odniesieniu do opracowywania zastosowań RFID w celu zapewnienia przestrzegania krajowego ustawodawstwa wdrażającego w stosownych przypadkach dyrektywy 95/46/WE, 1999/5/WE i 2002/58/WE przy wdrażaniu tych zastosowań.

Definicje

3. Do celów niniejszego zalecenia stosuje się definicje określone w dyrektywie 95/46/WE. Ponadto stosuje się następujące definicje:

a) „identyfikacja radiowa" (RFID) oznacza użycie fal promieniowania elektromagnetycznego lub sprzężenia strefy reaktancyjnej w części widma częstotliwości radiowej w celu przekazywania do identyfikatora lub od niego różnych schematów modulacji i kodowania, aby jednoznacznie odczytać tożsamość identyfikatora częstotliwości radiowej lub inne przechowywane w nim dane;

b) „identyfikator RFID" lub „identyfikator" oznacza urządzenie RFID zdolne do wytwarzania sygnału radiowego lub urządzenie RFID, które przekierowuje, rozprasza lub odbija (w zależności od typu urządzenia) i moduluje sygnał nośny otrzymany z czytnika lub urządzenia zapisującego;

c) „czytnik lub urządzenie zapisujące RFID" lub „czytnik" oznacza stacjonarne lub mobilne urządzenie przechwytujące i identyfikujące dane, wykorzystujące falę elektromagnetyczną częstotliwości radiowej lub sprzężenie strefy reaktancyjnej do stymulowania i wywoływania odpowiedzi zmodulowanych danych z identyfikatora lub grupy identyfikatorów;

d) „zastosowanie RFID" lub „zastosowanie" oznacza zastosowanie, które przetwarza dane przy pomocy identyfikatorów i czytników oraz jest wspierane systemem zaplecza i infrastrukturą sieci telekomunikacyjnej;

e) „operator zastosowania RFID" lub „operator" oznacza osobę fizyczną lub prawną, organ publiczny, agencję lub jakikolwiek inny podmiot, który samodzielnie lub wspólnie z innymi określa cele i środki działania zastosowania, włącznie z administratorami danych osobowych wykorzystującymi rozwiązania RFID;

f) „bezpieczeństwo informacji" oznacza zachowanie poufności, integralności i dostępności informacji;

g) „monitorowanie" oznacza jakąkolwiek działalność prowadzoną w celu wykrywania, obserwowania, kopiowania lub zapisywania położenia, ruchu, działań lub stanu osoby fizycznej.

Oceny skutków w zakresie ochrony danych i prywatności

4. Państwa członkowskie powinny zapewnić opracowanie przez sektor we współpracy z odpowiednimi zainteresowanymi stronami społeczeństwa obywatelskiego ram do ocen skutków w zakresie ochrony danych i prywatności. Ramy te należy przedłożyć do zatwierdzenia przez Grupę Roboczą ds. Ochrony Danych ustanowioną na mocy art. 29 w ciągu 12 miesięcy od opublikowania niniejszego zalecenia w *Dzienniku Urzędowym Unii Europejskiej*.

5. Państwa członkowskie powinny dopilnować, aby operatorzy niezależnie od swoich innych zobowiązań określonych w dyrektywie 95/46/WE:

a) przeprowadzali ocenę skutków wdrożenia zastosowań dla ochrony danych osobowych i prywatności, włącznie z ustaleniem, czy zastosowanie może być wykorzystane do monitorowania osoby fizycznej; poziom szczegółowości oceny powinien być odpowiedni dla czynników ryzyka dla prywatności, jakie mogłyby się wiązać z zastosowaniem;

b) podjęli odpowiednie środki techniczne i organizacyjne w celu zapewnienia ochrony danych osobowych i prywatności;

c) wyznaczyli osobę lub grupę osób odpowiedzialnych za przegląd ocen i utrzymania właściwego charakteru środków technicznych i organizacyjnych w celu zapewnienia ochrony danych osobowych i prywatności;

d) udostępnili ocenę właściwemu organowi co najmniej sześć tygodni przed wdrożeniem zastosowania;

e) wdrożyli powyższe przepisy zgodnie z ramami oceny skutków w zakresie ochrony danych i prywatności określonymi w pkt 4, gdy tylko będą one dostępne.

Bezpieczeństwo informacji

6. Państwa członkowskie powinny wspierać Komisję w identyfikacji tych zastosowań, które mogą powodować zagrożenia dla bezpieczeństwa informacji, mające skutki dla ogółu społeczeństwa. W przypadku takich zastosowań państwa członkowskie powinny dopilnować, aby operatorzy wraz z właściwymi organami krajowymi i organizacjami społeczeństwa obywatelskiego opracowali nowe systemy lub stosowali istniejące systemy, takie jak certyfikacja lub samoocena operatora w celu wykazania, że został ustanowiony odpowiedni poziom bezpieczeństwa informacji i ochrony prywatności w stosunku do ocenianych czynników ryzyka.

Zagadnienia informacji i przejrzystości w odniesieniu do stosowania RFID

7. Bez uszczerbku dla obowiązków administratorów danych i zgodnie z dyrektywami 95/46/WE i 2002/58/WE państwa członkowskie powinny dopilnować, aby operatorzy opracowali i opublikowali zwięzłe, dokładne i łatwe do zrozumienia informacje dotyczące każdego z ich zastosowań. Informacje te powinny obejmować co najmniej następujące elementy:

a) tożsamość i adres operatorów;

b) cel zastosowania;

c) informację o tym, jakie dane mają być przetwarzane przez zastosowanie, a w szczególności, czy przetwarzane będą dane osobowe, i czy położenie identyfikatorów będzie monitorowane;

d) streszczenie oceny skutków w zakresie ochrony danych i prywatności;

e) prawdopodobne ryzyko dla prywatności, jeśli takie występuje, związane z użyciem identyfikatorów w zastosowaniu, oraz środki, jakie osoby fizyczne mogą podjąć w celu zminimalizowana tego ryzyka.

8. Państwa członkowskie powinny zapewnić podjęcie przez operatorów kroków mających na celu informowanie osób fizycznych o obecności czytników przy pomocy wspólnego znaku europejskiego, opracowanego przez europejskie organizacje normalizacyjne przy wsparciu zainteresowanych stron. Znak powinien wskazywać tożsamość operatora i zawierać informacje na temat punktu kontaktowego dla osób fizycznych, w którym można uzyskać informacje dotyczące zastosowań.

Zastosowania RFID w sektorze handlu detalicznego

9. Na podstawie wspólnego znaku europejskiego, opracowanego przez europejskie organizacje normalizacyjne przy wsparciu zainteresowanych stron, operatorzy powinni informować osoby fizyczne o identyfikatorach umieszczonych na produktach lub wbudowanych w produkty.

10. Podczas przeprowadzania oceny skutków w zakresie ochrony danych i prywatności, o której mowa w pkt 4 i 5, operator zastosowania powinien szczegółowo określić, czy identyfikatory wbudowane w produkty lub umieszczone na produktach, które są sprzedawane konsumentom przez detalistów niebędących operatorami zastosowań, stanowią zagrożenie dla prywatności lub ochrony danych osobowych.

11. Detaliści powinni w punkcie sprzedaży dezaktywować lub usuwać identyfikatory używane w zastosowaniach, chyba że konsumenci, po udzieleniu im informacji, o których mowa w pkt 7, wyrażą zgodę na dalsze działanie identyfikatorów. Dezaktywację identyfikatorów należy rozumieć jako jakikolwiek proces wstrzymujący interakcję identyfikatora z jego środowiskiem, który nie wymaga aktywnego uczestnictwa konsumenta. Dezaktywacja lub usunięcie identyfikatorów przez detalistę powinny być natychmiastowe i bezpłatne. Konsumenci powinni mieć możliwość zweryfikowania, czy dezaktywacja lub usunięcie jest skuteczne.

12. Punkt 11 nie powinien mieć zastosowania, jeśli w wyniku oceny skutków w zakresie ochrony danych i prywatności okaże się, że identyfikatory używane w zastosowaniach obecnych w handlu detalicznym i działające nadal po opuszczeniu punktu sprzedaży nie stanowią zagrożenia dla prywatności lub ochrony danych osobowych. Mimo to detaliści powinni umożliwić bezpłatne i proste środki dezaktywacji lub usunięcia identyfikatorów natychmiast lub późniejszym terminie.

13. Dezaktywacja lub usunięcie identyfikatorów nie powinno wiązać się z jakimkolwiek ograniczeniem lub wygaśnięciem obowiązków prawnych detalisty lub producenta wobec konsumenta.

14. Punkty 11 i 12 powinny mieć zastosowanie tylko wobec detalistów, którzy są operatorami.

Działania podnoszące świadomość

15. Państwa członkowskie we współpracy z sektorem, Komisją i zainteresowanymi stronami powinny podjąć odpowiednie środki w celu informowania i podniesienia świadomości wśród organów publicznych i przedsiębiorstw (w szczególności małych i średnich) w zakresie potencjalnych korzyści i zagrożeń związanych ze stosowaniem technologii RFID. Należy zwrócić szczególną uwagę na aspekty dotyczące bezpieczeństwa informacji i prywatności.

16. Państwa członkowskie we współpracy z sektorem, organizacjami społeczeństwa obywatelskiego, Komisją i odpowiednimi zainteresowanymi stronami powinny określić i udostępnić przykłady dobrej praktyki we wdrażaniu zastosowań RFID na potrzeby informowania i podnoszenia świadomości społeczeństwa. Powinny one także podjąć odpowiednie środki, takie jak projekty pilotażowe na dużą skalę, aby podnieść świadomość społeczeństwa w zakresie technologii RFID oraz korzyści, zagrożeń i skutków wynikających z jej stosowania, co stanowi warunek wstępny szerszego wykorzystania tej technologii.

Badania i rozwój

17. Państwa członkowskie powinny współpracować z sektorem, odpowiednimi zainteresowanymi stronami społeczeństwa obywatelskiego i Komisją w celu pobudzania i wspierania wprowadzenia zasady „bezpieczeństwa i poszanowania prywatności od samego początku" na wczesnym etapie opracowywania zastosowań RFID.

Działania następcze

18. Państwa członkowskie powinny podjąć wszelkie niezbędne środki w celu przedstawienia niniejszego zalecenia wszystkim zainteresowanym stronom zaangażowanym w projektowanie i eksploatację zastosowań RFID we Wspólnocie.

19. Państwa członkowskie powinny poinformować Komisję o działaniach podjętych w odpowiedzi na niniejsze zalecenie najpóźniej 24 miesiące od opublikowania niniejszego zalecenia w *Dzienniku Urzędowym Unii Europejskiej*.

20. W ciągu trzech lat od opublikowania niniejszego zalecenia w *Dzienniku Urzędowym Unii Europejskiej* Komisja przedstawi sprawozdanie na temat wdrożenia niniejszego zalecenia, jego skuteczności i skutków dla operatorów i konsumentów, w szczególności w odniesieniu do środków zalecanych w punktach 9–14.

Adresaci

21. Niniejsze zalecenie skierowane jest do państw członkowskich.

Sporządzono w Brukseli, dnia 12 maja 2009 r.

W imieniu Komisji

Viviane REDING

Członek Komisji