GRUPA ROBOCZA DS. OCHRONY DANYCH USTANOWIONA NA MOCY ART. 29

00327/11/PL
WP 180

# Opinia 9/2011 na temat zmienionej propozycji sektora w sprawie ram oceny skutków w zakresie ochrony danych i prywatności w zastosowaniach RFID

**Przyjęta w dniu 11 lutego 2011 r.**

Grupa robocza została ustanowiona na mocy art. 29 dyrektywy 95/46/WE. Jest ona niezależnym europejskim organem doradczym w zakresie ochrony danych i prywatności. Zadania grupy określone są w art. 30 dyrektywy 95/46/WE i art. 15 dyrektywy 2002/58/WE.

Obsługę sekretariatu zapewnia Dyrekcja C (Prawa Podstawowe i Obywatelstwo Unii Europejskiej) Dyrekcji Generalnej ds. Sprawiedliwości, Wolności i Bezpieczeństwa Komisji Europejskiej, B-1049 Bruksela, Belgia, Biuro nr MO-59 06/36.

Strona internetowa: http://ec.europa.eu/justice/policies/privacy/index_en.htm

**Spis treści**

**GRUPA ROBOCZA DS. OCHRONY OSÓB FIZYCZNYCH W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH**

ustanowiona na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r.,

uwzględniając art. 29 i art. 30 ust. 1 lit. a) i ust. 3 tej dyrektywy oraz art. 15 ust. 3 dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r.,

uwzględniając swój regulamin,

**przyjmuje następującą opinię:**

# 1 Kontekst opinii

## *1.1 Wprowadzenie*

Opinia powstała w ramach działań następczych prowadzonych po wydaniu opinii[1] 5/2010 (WP 175) na temat „Propozycji sektora w sprawie ram oceny skutków w zakresie ochrony danych i prywatności w zastosowaniach RFID". Chociaż w niniejszym wprowadzeniu powtórzono niektóre elementy kontekstu niezbędne do zrozumienia celu i zakresu tej nowej opinii, informacje szczegółowe znajdują się w opinii 5/2010.

W dniu 12 maja 2009 r. Komisja Europejska wydała zalecenie[2] w sprawie wdrażania zasad ochrony prywatności i ochrony danych w zastosowaniach wspieranych identyfikacją radiową. We wspomnianym zaleceniu poproszono państwa członkowskie, aby zapewniły „opracowanie przez sektor we współpracy z odpowiednimi zainteresowanymi stronami (…) ram do oceny skutków w zakresie ochrony danych i prywatności", które miały być przedłożone „do zatwierdzenia przez Grupę Roboczą ds. Ochrony Danych ustanowioną na mocy art. 29". Po określeniu odnośnych ram oceny skutków w zakresie ochrony danych i prywatności, państwa członkowskie powinny zapewnić przeprowadzanie przez operatorów RFID oceny skutków w zakresie ochrony danych i prywatności w zastosowaniach RFID, zanim te zastosowania zostaną wprowadzone. Państwa członkowskie powinny także dopilnować, aby operatorzy RFID udostępnili właściwym organom sprawozdania będące wynikiem takiej oceny.

W dniu 31 marca 2010 r. przedstawiciele sektora przedłożyli grupie roboczej art. 29 do zatwierdzenia wniosek dotyczący ram oceny skutków w zakresie ochrony danych i prywatności. Chociaż propozycja ta stanowiła dobry punkt wyjścia, nie uzyskała pełnego poparcia grupy roboczej, zwłaszcza w związku z faktem, że w zaproponowanych ramach zabrakło trzech podstawowych elementów:

1) jasno zdefiniowanego podejścia w zakresie oceny ryzyka,

---

[1] Opinia 5/2010 na temat propozycji sektora w sprawie ram oceny skutków w zakresie ochrony danych i prywatności w zastosowaniach RFID, WP 175, 13 lipca 2010 r.

[2] http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf

2) uwzględnienia faktu noszenia identyfikatorów RFID przez osoby fizyczne poza granicami zastosowania tych identyfikatorów,

3) wyraźnego odniesienia się do zasad dezaktywacji identyfikatorów w sektorze detalicznym, ustanowionych w zaleceniu Komisji Europejskiej w sprawie wdrażania zasad ochrony prywatności i ochrony danych w zastosowaniach wspieranych identyfikacją radiową.

W dniu 13 lipca 2010 r. grupa robocza dokonała podsumowania tych elementów, a także innych kwestii w opinii 5/2010, zapraszając sektor do zaproponowania zmian do ram oceny skutków w zakresie ochrony danych i prywatności. Jeśli chodzi o samą ocenę ryzyka, grupa robocza zdecydowanie zachęciła sektor do wykorzystania wiedzy fachowej, jaką w tym obszarze dysponuje Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA).

W tym samym miesiącu ENISA opublikowała niezależną opinię[3] zawierającą praktyczne zalecenia dotyczące ulepszenia proponowanych ram. W swej opinii ENISA zaproponowała w szczególności pewne wstępne wytyczne dotyczące przyjęcia spójnego i uznawanego podejścia metodycznego do oceny ryzyka oraz zasugerowała kilka ulepszeń strukturalnych.

W kolejnych miesiącach sektor wprowadził zmiany do zrewidowanych ram oceny skutków w zakresie ochrony danych i prywatności, uwzględniające uwagi przekazane przez grupę roboczą i ENISA. W dniu 12 stycznia 2011 r. wspomniane zmienione ramy oceny skutków w zakresie ochrony danych i prywatności przedłożono do zatwierdzenia przez *Grupę Roboczą ds. Ochrony Danych ustanowioną na mocy art. 29.*

**Niniejsza opinia stanowi oficjalną odpowiedź grupy roboczej na odnośny nowy wniosek.**

W niniejszym dokumencie „zalecenie w sprawie RFID" odnosi się do zalecenia Komisji Europejskiej w sprawie wdrażania zasad ochrony prywatności i ochrony danych w zastosowaniach wspieranych identyfikacją radiową opublikowanego w dniu 12 maja 2009 r. „Zmienione ramy" lub „ramy" odnoszą się do ram oceny skutków w zakresie ochrony danych i prywatności w zastosowaniach identyfikacji radiowej (RFID) przekazanych grupie roboczej art. 29 w dniu 12 stycznia 2011 r. i odtworzonych w załączniku do niniejszej opinii.

## *1.2 Podsumowanie zmienionych ram*

Na początku zmienionych ram przedstawiono ważne procedury wewnętrzne związane z przeprowadzeniem oceny skutków w zakresie ochrony danych i prywatności i dotyczące m.in.: wyznaczenia terminu i dokonania przeglądu oceny skutków w zakresie ochrony danych i prywatności, sporządzenia stosownej dokumentacji, wyznaczenia w ramach organizacji osób odpowiedzialnych za wsparcie procesu oceny skutków w zakresie ochrony danych i prywatności, określenia warunków, które mogłyby spowodować zmianę oceny skutków w zakresie ochrony danych i prywatności w przyszłości oraz przeprowadzenia konsultacji z zainteresowanymi stronami.

Proces oceny skutków w zakresie ochrony danych i prywatności obejmuje dwie fazy:

[3] http://www.enisa.europa.eu/media/news-items/enisa-opinion-on-pia, Opinia ENISA na temat „Propozycji sektora w sprawie ram oceny skutków w zakresie ochrony danych i ochrony prywatności w zastosowaniach RFID" z 31 marca 2010 r.

I. fazę oceny wstępnej, w ramach której dokonuje się klasyfikacji zastosowania RFID według czterostopniowej skali na podstawie schematu podejmowania decyzji. Wynik tej oceny pozwala ustalić, czy ocena skutków w zakresie ochrony danych i prywatności jest potrzebna oraz dokonać wyboru między „pełną oceną skutków w zakresie ochrony danych i prywatności" a „niepełną oceną skutków w zakresie ochrony danych i prywatności". Zastosowania, w których wykorzystuje się identyfikatory RFID, które przypuszczalnie będą noszone przez osoby fizyczne, będą wymagać przeprowadzenia co najmniej „niepełnej oceny skutków w zakresie ochrony danych i prywatności" (poziom 1), zaś zastosowania, w ramach których dokonuje się dalszego przetwarzania danych osobowych będą wymagać przeprowadzenia „pełnej oceny skutków w zakresie ochrony danych i prywatności" (poziom 2 i 3). Odwrotnie, zastosowania w których nie wykorzystuje się identyfikatorów noszonych przez osoby fizyczne i w ramach których nie ma dalszego przetwarzania danych osobowych, nie podlegają ocenie skutków w zakresie ochrony danych i prywatności (poziom 0).
II. fazę oceny ryzyka, która dzieli się na cztery główne etapy:
    1) charakterystykę zastosowania (rodzaje danych, przepływy danych, technologia RFID, przechowywanie i transfery danych itp.);
    2) identyfikację rodzajów ryzyka związanego z danymi osobowymi poprzez ocenę zagrożeń, prawdopodobieństwa ich wystąpienia oraz wpływu, jeśli chodzi o prywatność i zgodność z prawodawstwem europejskim;
    3) określenie rodzajów kontroli oraz sformułowanie zaleceń dotyczących ich przeprowadzania, jako odpowiedź na uprzednio zidentyfikowane rodzaje ryzyka;
    4) udokumentowanie wyników oceny skutków w zakresie ochrony danych i prywatności, znalezienie rozwiązania dotyczącego warunków wdrożenia ocenianego zastosowania RFID oraz informowanie o pozostałym ryzyku.

Na każdym etapie fazy oceny ryzyka zapewnia się dodatkowe wsparcie w postaci elementów przedstawionych w załącznikach do zmienionych ram, które mają także służyć jako wskazówki dla osoby przeprowadzającej ocenę. Należą do nich:

- wzór, który umożliwia przedstawienie głównych cech charakterystycznych zastosowania RFID;
- wykaz dziewięciu celów w zakresie prywatności dla zastosowania RFID, wywodzących się z dyrektywy 95/46/WE;
- wykaz typowych zagrożeń dla prywatności, wraz z opisami i przykładami;
- wykaz przykładów kontroli i środków ograniczających ryzyko, które można wykorzystać w odpowiedzi na uprzednio zidentyfikowane ryzyko.

Wynik oceny skutków w zakresie ochrony danych i prywatności przyjmuje oficjalną formę sprawozdania z oceny skutków w zakresie ochrony danych i prywatności, przygotowanego przez operatora zastosowania RFID, które zawiera opis zastosowania RFID oraz dokumentuje szczegóły wspomnianych powyżej czterech etapów oceny ryzyka.

# 2 Analiza

Grupa robocza przyjmuje z aprobatą dogłębną analizę zagadnienia przeprowadzoną w ostatnich miesiącach przez stowarzyszenia branżowe i ekspertów branżowych oraz

naukowców i indywidualne przedsiębiorstwa, którzy opracowali zmienione ramy. Autorzy ram, przy okazji wprowadzania omawianych zmian, podjęli wysiłek nie tylko poradzenia sobie z większością problemów uwypuklonych przez grupę roboczą, ale także przedstawienia jasnej struktury i dokładniejszych wytycznych dla operatorów RFID, którzy będą wdrażać te ramy.

Grupa robocza zwraca uwagę, że zmienione ramy opracowano na podstawie podejścia opartego na zarządzaniu ryzykiem i ponownie podkreśla, że stanowi ono istotny składnik wszystkich ram oceny skutków w zakresie ochrony danych i prywatności.

Grupa robocza przyjmuje ponadto z aprobatą wyraźne włączenie procesu konsultacji z zainteresowanymi stronami do procedur wewnętrznych koniecznych do wsparcia oceny skutków w zakresie ochrony danych i prywatności.

Proponowana metoda oceny ryzyka rozpoczyna się od schematu podejmowania decyzji w fazie oceny wstępnej, który klasyfikuje zastosowania RFID do jednego z czterech poziomów. Grupa robocza zauważa, że w proponowanym schemacie podejmowania decyzji nie jest jasne, jaki rodzaj danych można uznać za dane osobowe w zastosowaniu RFID. Jeśli identyfikator zawierający niepowtarzalne dane identyfikacyjne ma nosić osoba fizyczna, wtedy dane identyfikacyjne identyfikatora należy uznać za dane osobowe, jak podkreślono uprzednio w opinii 5/2010. Tak więc w większości sytuacji, jeśli identyfikator ma nosić osoba fizyczna, będzie się on kwalifikować jako zastosowanie poziomu 2, a nie zastosowanie poziomu 1, jak wynikałoby z ram. Niemniej jednak grupa robocza z aprobatą przyjmuje fakt, że zmienione ramy jasno wymagają od operatorów RFID, aby przeprowadzali ocenę skutków w zakresie ochrony danych i prywatności za każdym razem, gdy identyfikator nosi osoba fizyczna.

Jak opisano w kilku wcześniejszych opiniach[4], jeden z głównych problemów w zakresie ochrony prywatności, związanych z technologią RFID**,** „wiąże się z wykorzystywaniem technologii RFID, które obejmują śledzenie osób i uzyskiwanie dostępu do danych osobowych". Chociaż operator RFID, wprowadzając zastosowanie RFID, może nie kierować się tym celem, należy wziąć pod uwagę ryzyko, że osoba trzecia może wykorzystać identyfikatory do takich niezamierzonych celów. Zmienione ramy wyraźnie wymagają od operatorów RFID dokonania oceny ryzyka, jakie może wiązać się z wykorzystaniem identyfikatorów poza granicami zastosowania RFID lub noszeniem ich przez osoby fizyczne.

Na problem ten zwrócił szczególną uwagę sektor detaliczny, którego przedstawiciele obawiają się, że przedmioty z identyfikatorem kupowane przez osoby fizyczne mogłyby być niewłaściwie wykorzystane przez detalistów lub osoby trzecie do celów śledzenia lub opracowywania profili. Komisja Europejska zajęła się tym problemem w wydanym przez siebie zaleceniu, ustalając zasadę, zgodnie z którą identyfikatory muszą być dezaktywowane w punkcie sprzedaży, chyba że konsumenci wyrażą świadomą zgodę na dalsze działanie identyfikatorów. W tym samym zaleceniu zezwala się na wyjątek od tej zasady dezaktywacji w przypadku, gdy ocena skutków w zakresie ochrony danych osobowych i prywatności wykaże, że dalsze działanie identyfikatorów po opuszczeniu punktu sprzedaży nie wiąże się z „prawdopodobieństwem zagrożenia dla prywatności lub ochrony danych osobowych". Grupa robocza zauważa, że podejście do zarządzania ryzykiem, jak sugeruje się w ramach, stanowi istotne narzędzie

[4] Zob. na przykład opinia 5/2010 (WP 175) i WP 105 „Dokument roboczy na temat kwestii zakresu ochrony danych związanych z technologią RFID", 19 stycznia 2005 r.

przeprowadzenia przez operatora RFID oceny ryzyka przyjęcia odpowiedzialności za dalsze działanie identyfikatorów po opuszczeniu punktu sprzedaży.

Na zakończenie oceny skutków w zakresie ochrony danych osobowych i prywatności powstanie sprawozdanie z oceny skutków tej oceny, które zostanie następnie udostępnione właściwym organom co najmniej sześć tygodni przed wdrożeniem zastosowania RFID. Grupa robocza pragnie podkreślić, że przeprowadzenie oceny skutków w zakresie ochrony danych osobowych i prywatności będzie także wymagać od operatorów RFID, aby „opracowali i opublikowali zwięzłe, dokładne i łatwe do zrozumienia informacje dotyczące każdego z zastosowań (jak opisano w pkt 7 zalecenia). Informacje te powinny zwłaszcza uwzględniać „streszczenie oceny skutków w zakresie ochrony danych i prywatności".

W związku z faktem, że rozpoczyna się już proces wdrażania ram do konkretnych zastosowań RFID, ich treść będzie prawdopodobnie wymagać korekt, które mogą opierać się wyłącznie na wiedzy specjalistycznej i komentarzach wszystkich zainteresowanych stron, w tym sektora, konsumentów, organów ds. ochrony danych i ENISA. Będzie to prawdopodobnie dotyczyć w szczególności rozróżnienia między „pełną" a „niepełną"oceną skutków w zakresie ochrony danych osobowych i prywatności, zgodnie z odnośnymi definicjami w zmienionych ramach. Ponadto, zgodnie z zaleceniem, Komisja Europejska ma przedstawić „sprawozdanie na temat wdrożenia zalecenia, jego skuteczności i skutków dla operatorów i konsumentów", w szczególności w odniesieniu do środków dotyczących sektora detalicznego. Sprawozdanie to ma być przygotowane w ciągu trzech lat od opublikowania zalecenia, czyli do maja 2012 r. Jednak w związku z faktem, że zapewnienie pełnej skuteczności ram może potrwać sześć miesięcy, korzystne dla wszystkich zainteresowanych stron byłoby wyznaczenie okresu dodatkowego poprzedzającego ocenę. Grupa robocza pragnie zatem zasugerować, aby Komisja Europejska przesunęła termin przedłożenia proponowanego sprawozdania na czas późniejszy niż trzy lata od opublikowania niniejszej opinii lub też aby uzupełniła je w tym terminie.

# 3 Wniosek

Grupa robocza zatwierdza zmienione ramy przedłożone w dniu 12 stycznia 2011 r. Ramy te stają się skuteczne nie później niż w ciągu sześciu miesięcy od opublikowania niniejszej opinii.

Ramy oceny skutków w zakresie ochrony danych i prywatności są narzędziem mającym na celu promowanie „zasadę domyślnej ochrony prywatności", lepszego informowania osób fizycznych, a także przejrzystości i dialogu z właściwymi organami. Z tego względu, w związku z faktem że zastosowania RFID będą podlegać wdrożeniu w wielu państwach członkowskich, niezbędne jest przetłumaczenie sprawozdań z oceny skutków w zakresie ochrony danych i prywatności oraz udostępnienie wspomnianych sprawozdań właściwym organom w ich językach krajowych.

Grupa robocza zamierza nadal wspierać dialog, który będzie w przyszłości prowadzony z sektorem, jeśli chodzi o ulepszenia i objaśnienia struktury i sposobu wdrożenia zmienionych ram oceny skutków w zakresie ochrony danych i prywatności w zastosowaniach RFID, wspierany wiedzą fachową i komentarzami wszystkich zainteresowanych stron.