Grupa robocza art. 29

00066/10/PL
WP 175

Opinia 5/2010 na temat propozycji sektora w sprawie ram oceny skutków w zakresie ochrony danych i prywatności w zastosowaniach RFID

Przyjęta w dniu 13 lipca 2010 r.

Spis treści

1 Kontekst opinii

1.1 Wprowadzenie

W dniu 12 maja Komisja Europejska wydała zalecenie w sprawie wdrażania zasad ochrony prywatności i ochrony danych w zastosowaniach wspieranych identyfikacją radiową[1].

W punkcie 4 wymienionego zalecenia stwierdza się, że: *„Państwa członkowskie powinny zapewnić opracowanie przez sektor, we współpracy z odpowiednimi zainteresowanymi podmiotami społeczeństwa obywatelskiego, ram 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*" (podkreślenia dodano).

Zgodnie z wymienionym zaleceniem, po określeniu odnośnych ram ocen skutków w zakresie ochrony danych i prywatności, państwa członkowskie powinny zapewnić przeprowadzanie przez operatorów RFID oceny skutków w zakresie ochrony danych i prywatności (PIA) w zastosowaniach RFID zanim te zastosowania zostaną wprowadzone. Państwa członkowskie powinny także zapewnić, że operatorzy RFID udostępnią właściwym organom, tj. organom ds. ochrony danych (ang. *DPA – data protection authorities*), sprawozdania będące wynikiem takiej oceny.

W lipcu 2009 r. nieformalna grupa robocza ds. RFID kierowana przez przedstawicieli odnośnego sektora rozpoczęła pracę nad określeniem ram oceny skutków w zakresie ochrony danych i prywatności, odbywając jednocześnie regularne posiedzenia z zainteresowanymi stronami, w tym grupami konsumentów, organami normalizacyjnymi i akademickimi pracownikami naukowymi. W dniu 31 marca 2010 r. przedstawiciele sektora przedłożyli grupie roboczej art. 29 w celu zatwierdzenia wniosek dotyczący ram ocen skutków w zakresie ochrony danych i prywatności. **Niniejsza opinia stanowi oficjalną odpowiedź grupy roboczej na odnośny 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. „Proponowane 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 31 marca 2010 r. i odtworzonych w załączniku do niniejszej opinii.

1.2 RFID i ochrona danych

W styczniu 2005 r. grupa robocza przyjęła *dokument roboczy*[2] *w sprawie zagadnień dotyczących technologii RFID* (WP 105), w którym potwierdza się ewidentne korzyści, jakie oferuje technologia RFID, lecz także podkreśla się ewentualne problemy w dziedzinie ochrony danych, które mogą powstać

[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

przede wszystkim w wyniku *„możliwości wykorzystania technologii RFID przez przedsiębiorstwa i instytucje rządowe w celu ingerowania w sferę prywatności osób fizycznych”*. W wymienionym dokumencie podkreśla się, że *„możliwość potajemnego zgromadzenia całego zbioru różnorodnych danych dotyczących jednej osoby, śledzenia osób przebywających w miejscach publicznych (na lotniskach, stacjach kolejowych, w sklepach), opracowywania profili poprzez monitorowanie zachowań konsumenckich w sklepach, odczytywania szczegółowych informacji o ubraniach i akcesoriach noszonych przez klientów, a także posiadanych przez nich lekach – to wszystko są przykłady wykorzystania technologii RFID, które dają podstawy do obaw w zakresie ochrony prywatności.”*

Odnośny dokument roboczy przedstawiono następnie do konsultacji publicznej. Wynik tego procesu podsumowano w dokumencie (WP 111)[3] opublikowanym przez grupę roboczą we wrześniu 2005 r. Wyniki pokazały, że podczas gdy „*większość uniwersytetów, ośrodków analitycznych, osób prywatnych i przedsiębiorstw dostarczających rozwiązania w zakresie bezpieczeństwa zasugerowało potrzebę udzielenia przez grupę roboczą art. 29 pewnego rodzaju dodatkowych wytycznych*”, a niektórzy zaproponowali „u*zupełnienie dyrektywy o ochronie danych o szczególne wytyczne w zakresie RFID*”, sektor prosił o „*podejście samoregulacyjne*”.

W takim kontekście i we współpracy z zainteresowanymi stronami, w tym przedstawicielami sektora RFID, organizacjami praw konsumentów i ochrony danych, Komisja Europejska podjęła inicjatywę w opracowaniu zalecenia[4] *„w sprawie wdrażania zasad ochrony prywatności i ochrony danych w zastosowaniach wspieranych identyfikacją radiową”* mającego na celu udzielenie *„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”*.

Wspomniane zalecenie, opublikowane w maju 2009 r., zawiera istotną nowość: wymaga, aby operatorzy RFID przeprowadzali „ocenę skutków w zakresie ochrony danych i prywatności” przed wprowadzeniem zastosowania RFID oraz udostępniali wyniki takiej oceny właściwym organom. To nowe podejście, będące uzupełnieniem obowiązujących ram prawnych przewidzianych w dyrektywie o ochronie danych i dyrektywie o prywatności i łączności elektronicznej, zapewnia sektorowi możliwość wykazania, że potencjał samoregulacji stanowi uzupełniające, elastyczne i skuteczne narzędzie ram prawnych UE w obliczu szybko zmieniającego się krajobrazu technologicznego. Grupa robocza wspiera[5] *„przeprowadzanie ocen skutków w zakresie prywatności, w szczególności w przypadku pewnych procesów przetwarzania danych, które mogą być postrzegane jako przedstawiające określone zagrożenia dla praw i wolności osób, których dane dotyczą”*. Grupa robocza uważa także, że sukces lub porażka w przypadku takiego podejścia prawdopodobnie albo przetrą szlaki dla wykorzystania ocen skutków w zakresie ochrony danych i prywatności w innych dziedzinach, albo też spowodują wzmocnione podejście regulacyjne.

---

3 *„Wyniki konsultacji publicznej w sprawie roboczego dokumentu 105 grupy roboczej art. 29 dotyczącego zagadnień ochrony danych w powiązaniu z technologią RFID”(ang. „Results of the Public Consultation on Article 29 Working Document 105 on Data Protection Issues Related to RFID Technology”)*, 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 Zob.: „The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data”, WP 168, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp168_en.pdf

Zalecenie w sprawie RFID ma promować „*informację i przejrzystość w odniesieniu do stosowania RFID"*, w szczególności poprzez opracowanie *„wspólnego znaku europejskiego, opracowanego przez europejskie organizacje normalizacyjne przy wsparciu zainteresowanych stron*", wprowadzonego w celu *„informowania osób fizycznych o obecności czytników"*. Taka inicjatywa cieszy się pełnym poparciem grupy roboczej.

Pomimo że zalecenie w sprawie RFID wyraźnie odnosi się do dyrektywy 95/46/WE, w pewnych przypadkach czerpie z terminologii zwyczajowo stosowanej w przepisach dotyczących ochrony danych, w szczególności w odniesieniu do „osób", „osób fizycznych" lub „użytkowników". Aby uniknąć niejasności, w niniejszej opinii słowo „osoba" (*person*), odnosi się do osoby fizycznej zgodnie z art. 2 dyrektywy 95/46/WE, a słowa „Użytkownik" (*User*) i „Osoba fizyczna" (*Individual*) pisane wielką literą zachowają to samo znaczenie co w zaleceniu w sprawie RFID. W szczególności słowo „osoba" może być używane zarówno w stosunku do „Użytkowników" jak i „Osób fizycznych", które w innym ujęciu stanowią odrębne kategorie osób, zgodnie z definicjami określonymi w pkt. 3 zalecenia w sprawie RFID, które powtarza się w proponowanych ramach. Aby zachować spójność z zaleceniem w sprawie RFID, niniejsza opinia będzie także odnosić się do „operatorów RFID", a nie „administratorów danych", mimo że oba te terminy nie są całkowicie równoważne.

W listopadzie 2009 r. prawodawcy europejscy zmienili dyrektywę o prywatności i łączności elektronicznej[6], odnosząc się w sposób wyraźny do technologii RFID. W motywie 56 dyrektywy 2009/136/WE stwierdzili oni, że *„zastosowanie tego rodzaju technologii na szeroką skalę może przynieść istotne korzyści gospodarcze i społeczne, a tym samym w znaczący sposób przyczynić się do urzeczywistnienia rynku wewnętrznego, jeżeli ich stosowanie zostanie zaakceptowane przez obywateli"*, jak również, że *„aby osiągnąć ten cel, należy zapewnić ochronę wszystkich podstawowych praw jednostek, w tym prawa do prywatności i ochrony danych"*. Ponadto dodali w dyrektywie, że *„w przypadku gdy takie urządzenia są przyłączone do publicznie dostępnych sieci łączności elektronicznej lub korzystają z usług łączności elektronicznej jako podstawowej infrastruktury, zastosowanie mają odpowiednie przepisy dyrektywy 2002/58/WE (dyrektywa o prywatności i łączności elektronicznej), wraz z przepisami dotyczącymi bezpieczeństwa, ruchu i danych dotyczących lokalizacji oraz przepisami dotyczącymi poufności."* W rezultacie zakres dyrektywy o prywatności i łączności elektronicznej (określony w art. 3) został zmieniony tak, aby *uwzględnić „publiczne sieci łączności służące do zbierania danych i obsługi urządzeń identyfikacyjnych"*.

1.3 Cele ram oceny skutków w zakresie ochrony danych i prywatności

Za pomocą zalecenia RFID Komisja Europejska utworzyła proces oceny skutków w zakresie ochrony danych i prywatności, który ma na celu osiągnięcie kilku korzyści:

- Po pierwsze, ocena skutków w zakresie ochrony danych i prywatności powinna sprzyjać „poszanowaniu prywatności od samego początku", pomagając administratorom danych

[6] Dyrektywa Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r. zmieniająca dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenie (WE) nr 2006/2004 w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów.

uwzględnić ochronę danych i prywatności przed wprowadzeniem produktu lub usługi. Takie działanie przynosi korzyści nie tylko osobom fizycznym, ale także administratorom danych, pozwalając na uniknięcie wysokich kosztów (i często niesatysfakcjonujących rozwiązań), które nierzadko pojawiają się, gdy trzeba dołączyć elementy dotyczące ochrony prywatności do produktu już wprowadzonego na rynek.

- Po drugie, ocena skutków w zakresie ochrony danych i prywatności powinna pomóc administratorom danych odnieść się do kwestii zagrożeń związanych z ochroną danych i prywatności w sposób kompleksowy. Ocena skutków w zakresie ochrony danych i prywatności stanowi część narzędzi, które mogą pomóc w dokonaniu oceny ryzyka dla prywatności i znalezieniu środków technicznych i organizacyjnych w celu ochrony danych osobowych przed niedozwolonym ujawnieniem lub dostępem, oraz aby objąć inne zobowiązania w odniesieniu do bezpieczeństwa ustanowione w art. 17 dyrektywy o ochronie danych i art. 4 zmienionej dyrektywy 2002/58. Taki proces daje także możliwość zmniejszenia niepewności prawnej i uniknięcia utraty zaufania ze strony opinii publicznej, która w przeciwnym wypadku mogłaby stanowić obciążenie dla administratora danych, gdyby kwestie ochrony danych nie zostały właściwie rozwiązane.

- Po trzecie, oceny skutków w zakresie ochrony danych i prywatności mogą pomóc zarówno administratorom danych, jak i organom ochrony danych uzyskać lepszy ogląd istoty zagadnienia ochrony danych i prywatności w zastosowaniach RFID. Przeprowadzenie oceny skutków w zakresie ochrony danych i prywatności powinno pomóc administratorom danych w zrozumieniu i zastosowaniu zasad ustanowionych w dyrektywie 95/46/WE, dyrektywie 2002/58/WE, która została niedawno zmieniona, oraz w zaleceniu w sprawie RFID. Informacja uzyskana w wyniku przeprowadzenia oceny skutków w zakresie ochrony danych i prywatności może pomóc organom ochrony danych określić najlepsze praktyki wdrażania ochrony danych przez sektor, a w tych państwach członkowskich, w których wymagana jest wcześniejsza kontrola (części lub wszystkich) zastosowań RFID, może ona ułatwić ten proces organom ochrony danych i administratorów danych[7].

Ponadto grupa robocza uważa opracowanie oceny skutków w zakresie ochrony danych i prywatności za istotny czynnik sprzyjający konkurencyjności przemysłu europejskiego RFID, który wspiera innowacyjne metody rozwiązywania problemów w zakresie ochrony danych i prywatności za pomocą technologii takich jak anonimizacja danych, częściowa dezaktywacja identyfikatorów, „lekka" kryptografia (ang. *lightweight cryptography*) itp.

Pomimo że ramy oceny skutków w zakresie ochrony danych i prywatności przewidziane w zaleceniu mają na celu promowanie „bezpieczeństwa i poszanowania prywatności od samego początku" poprzez koncentrowanie się na zastosowaniach RFID przed ich wprowadzeniem, to istnieje już wiele wprowadzonych zastosowań RFID. Grupa robocza ma nadzieję, że zainteresowane strony będą czerpać z

[7] W tym kontekście, pkt. 5 lit d) zalecenia w sprawie RFID stanowi, że operatorzy niezależnie od swoich innych zobowiązań określonych w dyrektywie 95/46/WE powinni udostępnić ocenę właściwemu organowi co najmniej sześć tygodni przed wdrożeniem zastosowania. Sposób w jaki należy udostępnić ocenę skutków w zakresie ochrony danych i prywatności (np. na wniosek lub bez wniosku) zostanie określony przez krajowe organy ochrony danych. Przede wszystkim, pod uwagę można wziąć zagrożenie związane z zastosowaniem oraz inne czynniki takie jak obecność urzędnika do spraw ochrony danych osobowych.

tego doświadczenia i wykorzystają tę okazję do opracowania narzędzi oceny, które mogą być stosowane w istniejących zastosowaniach RFID.

1.4 Podsumowanie proponowanych ram

Proponowane ramy najpierw klasyfikują zastosowania RFID, ustanawiając cztery możliwe poziomy. Zastosowania „poziomu 0" obejmujące zasadniczo zastosowania RFID, które nie przetwarzają danych osobowych i w których użytkownicy jedynie posługują się identyfikatorami, są wyłączone z przeprowadzania oceny skutków w zakresie ochrony danych i prywatności. Słowo „Użytkownik" może potencjalnie obejmować pracowników, nie można przez to jednak rozumieć, że definicja poziomu 0 obejmuje zastosowanie, które ma na celu monitorowanie pracowników, ponieważ takie monitorowanie wymagałoby przechowywania danych osobowych w jakimś miejscu aplikacji. W związku z tym grupa robocza zgadza się, że nie jest prawdopodobne, aby wyłączenie „zastosowań poziomu 0" z procesu oceny skutków w zakresie ochrony danych i prywatności miało niekorzystne skutki dla celów ochrony danych i prywatności.

Zastosowania poziomu 1 obejmują zastosowania, w których nie przetwarza się danych osobowych, jednak identyfikatory noszą Osoby fizyczne. Zastosowania poziomu 2 to zastosowania, które przetwarzają dane osobowe, ale w których identyfikatory jako takie nie zawierają danych osobowych. Zastosowania poziomu 3 natomiast to zastosowania, w których identyfikatory zawierają dane osobowe. Jak podkreślono w sekcji 2.4 poniżej, użycie terminu „dane osobowe" jest nieco dwuznaczne w proponowanych ramach w odniesieniu do informacji zawartych w identyfikatorach.

Jeżeli poziom zastosowania RFID określa się jako 1 lub wyższy niż 1, wymaga się, aby operator RFID przeprowadził czteroczęściową analizę zastosowania o poziomie szczegółowości proporcjonalnym do zidentyfikowanych skutków dla prywatności i ochrony danych. W pierwszej części opisuje się zastosowanie RFID. Druga część pozwala na podkreślenie środków kontroli i bezpieczeństwa. Trzecia część dotyczy informacji dla użytkownika i jego praw. Ostatnia część proponowanych ram oceny skutków w zakresie ochrony danych i prywatności wymaga, by operator RFID podsumował, czy zastosowanie RFID jest gotowe do wprowadzenia. W wyniku procesu oceny skutków w zakresie ochrony danych i prywatności operator RFID przygotuje sprawozdanie w sprawie oceny skutków w zakresie ochrony danych i prywatności, które zostanie udostępnione właściwemu organowi.

Ze względu na pewne szczególne potrzeby sektora autorzy proponowanych ram zakładają, że sektor może przełożyć ramy na konkretne „wzory do przeprowadzania oceny skutków w zakresie ochrony danych i prywatności ", aby ułatwić zastosowanie tych ram. „Sprawozdanie z oceny skutków w zakresie ochrony danych i prywatności" powstanie zatem w oparciu o konkretny wzór dla danego sektora, a nie ogólne ramy.

2 Analiza

Grupa robocza przyjmuje z aprobatą szeroko zakrojone prace przeprowadzone przez autorów proponowanych ram i zgadza się z głównymi celami podkreślonymi w sekcjach wstępnych.

Całościowy zarys proponowanych ram nie budzi szczególnych zastrzeżeń, jednak w odniesieniu do ich treści grupa robocza wyszczególniła trzy istotne kwestie budzące wątpliwość, oraz kilka uwag, które przedstawiono poniżej.

2.1 Ocena ryzyka

We wstępie do proponowanych ram jednoznacznie stwierdza się, że *„proces oceny skutków w zakresie ochrony danych i prywatności ma na celu ujawnienie zagrożenia prywatności związanego ze stosowaniem RFID* […] *i ocenę kroków podjętych w celu przeciwdziałania temu zagrożeniu”*. **Jednak to główne założenie w odniesieniu do procesu oceny skutków w zakresie ochrony danych i prywatności nie ma swojego odzwierciedlenia w treści proponowanych ram.**

Proponowane ramy odnoszą się co prawda w pewnych miejscach do oceny ryzyka (szczególnie w częściach wstępnych), jednak żadna z sekcji nie zawiera wyraźnego wymogu, aby operator RFID określił lub *„ujawnił zagrożenie prywatności związane ze stosowaniem RFID”.* W związku z tym niemożliwe jest także *„dokonanie oceny kroków podjętych w celu przeciwdziałania temu zagrożeniu”*. Proponowane ramy wymagają jedynie, aby operator RFID wymienił różne zabezpieczenia i kontrole, które zostały wprowadzone w celu ochrony danych osobowych i prywatności w zastosowaniach RFID. Nie można tego uznać za satysfakcjonujący środek, który dałby operatorowi RFID lub właściwym organom rozsądną gwarancję, że zaproponowane środki są odpowiednie lub proporcjonalne do zagrożeń, ponieważ zagrożenia te nie zostały wcześniej zidentyfikowane.

Grupa robocza wyraża głębokie ubolewanie, że autorzy proponowanych ram nie odnieśli się do tej kwestii.

Co do zasady, ramy oceny skutków w zakresie ochrony danych i prywatności powinny proponować ogólną metodykę obejmującą etap oceny ryzyka jako elementu kluczowego. Sektor RFID z pewnością stosuje już oceny ryzyka jako część podejścia metodycznego w kontekście zarządzania bezpieczeństwem informacji, tak jak określono w ISO/IEC 27005[8] i w innych normach krajowych i międzynarodowych. Grupa robocza jest przekonana, że sektor RFID może wykorzystać tę specjalistyczną wiedzę w dziedzinie tradycyjnego zarządzania bezpieczeństwem informacji w celu wzbogacenia proponowanych ram o, mające szczególne znaczenie, podejście w zakresie oceny ryzyka. Miałoby to wpływ na inne szczególne elementy proponowanych ram, jak podkreślono zwłaszcza w sekcjach 2.2, 2.3 i 2.4 niniejszej opinii.

Ponadto w motywie 17 zalecenia w sprawie RFID zauważa się, że opracowanie ram oceny skutków w zakresie ochrony danych i prywatności *„powinno opierać się na istniejących praktykach i doświadczeniach zdobytych w państwach członkowskich, w krajach trzecich i w ramach prac*

[8] Zob.: ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems – Requirements.

prowadzonych przez Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji (ENISA)". Daje to prawomocny mandat autorom proponowanych ram rozważenia przyjętej ostatnio przez ENISA opinii na temat ram oceny skutków w zakresie ochrony danych i prywatności[9] i wymaga dalszych wskazówek ze strony agencji UE w sprawie stosowania podejścia w zakresie oceny ryzyka w kontekście RFID. ENISA w sposób szczególny podjęła się[10] *„zadania określenia i oceny powstających i przyszłych zagrożeń dotyczących szczególnego scenariusza „Internet przedmiotów/RFID", zwłaszcza w kontekście roli ENISA w wyszczególnionym w komunikacie WE „Internet przedmiotów – plan działań dla Europy"*[11]. **Grupa robocza zdecydowanie zachęca sektor do wykorzystania tej możliwości.**

2.2 Identyfikatory noszone przez osoby

Jeden z trzech głównych problemów związanych z ochroną prywatności, podkreślonych w *„dokumencie roboczym na temat kwestii z zakresu ochrony danych związanych w technologią RFID"* (WP 105)[12], *„wiąże się z wykorzystaniem technologii RFID, które obejmują śledzenie osób i uzyskiwanie dostępu do danych osobowych"*. ‚Przedmioty z identyfikatorem noszone przez osobę zawierają niepowtarzalne znaczniki, które można odczytać w sposób zdalny. Z kolei te niepowtarzalne znaczniki można wykorzystywać do rozpoznawania danej osoby w czasie w sposób ciągły, czyniąc ją „możliwą do zidentyfikowania". W pewnych przypadkach może być to pożądane, w szczególności, gdy przedmiot z identyfikatorem został zaprojektowany do użycia jako mechanizm kontroli dostępu (np. identyfikator zezwalający na wstęp do budynku). W pozostałych przypadkach jednak daje to możliwość śledzenia[13] osoby bez jej wiedzy przez stronę trzecią. Zgodnie z tym, co podkreślono w *„Opinii 4/2007 w sprawie pojęcia danych osobowych"* (WP 136)[14], kiedy unikalny znacznik jest kojarzony z osobą, objęty jest definicją o danych osobowych ustanowioną w dyrektywie 95/46/WE, bez względu na fakt, że „tożsamość społeczna" (nazwisko, adres itp.) osoby pozostają nieznane (np. osoba jest „możliwa do zidentyfikowania" ale niekoniecznie „zidentyfikowana").

Ponadto niepowtarzalny numer, który zawiera identyfikator, może także służyć jako środek do zdalnego identyfikowania charakteru przedmiotu, który posiada osoba, co z kolei może ujawnić informacje o statusie społecznym, zdrowiu lub inne. Zatem jeśli identyfikator ma być noszony przez osoby, to nawet w przypadkach, gdy identyfikator zawiera jedynie numer, który jest niepowtarzalny w danym kontekście, i nie zawiera żadnych dodatkowych danych osobowych, należy podjąć kroki dotyczące potencjalnych kwestii bezpieczeństwa i poszanowania prywatności.

Grupa robocza z aprobatą przyjmuje fakt, że sektor ujął ten problem w ramach oceny skutków w zakresie ochrony danych i prywatności, wymagając przeprowadzenia takiej oceny, gdy *„identyfikatory poziomu przedmiotu przeznacza się do noszenia przez osoby fizyczne"*(zastosowania „poziomu 1").

---

9 Opinia ENISA na temat propozycji sektora w sprawie ram oceny skutków w zakresie ochrony danych i ochrony prywatności w zastosowaniach RFID, lipiec 2010 r., http://www.enisa.europa.eu/media/news-items/enisa-opinion-on-pia

10 Zob. np. sprawozdanie ENISA pt. „Flying 2.0 - Enabling automated air travel by identifying and addressing the challenges of IoT & RFID technology".

11 Komisja Europejska, Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Internet przedmiotów – plan działań dla Europy, COM(2009) 278, Bruksela, 18.6.2009 r.

12 Zob. przypis 2.

13 Zob. przykłady podane w WP 105, sekcja 3.3.

14 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf

Niestety pomimo takiego założenia **proponowane ramy** nie odnoszą się do tej kwestii **i nie zachęcają w sposób wyraźny operatora RFID do dokonania oceny problemów dotyczących ochrony danych i prywatności, które mogłyby wyniknąć, gdyby w życiu codziennym identyfikatory były noszone przez osoby fizyczne**. Nie wystarczy rozważyć, *„czy za pomocą zastosowania RFID będzie monitorowana lokalizacja Osób fizycznych lub Użytkowników”*[15]. Bardzo ważne jest także, aby przeanalizować ryzyko niedozwolonego monitorowania wykraczającego poza granice zastosowania. Ramy nie opisują również kroków podjętych w celu przeciwdziałania takiemu zagrożeniu. **Grupa robocza wzywa sektor do rozwiązania tego problemu poprzez wyraźne wymienienie go w ramach jako część zmienionego podejścia w zakresie oceny ryzyka.**

2.3 RFID w sektorze detalicznym

Jednym z kluczowych obszarów zastosowań, w którym identyfikatory mogłyby nosić osoby fizyczne, jest sektor detaliczny. Zalecenie w sprawie RFID uznaje ten sektor za najważniejszy i odnosi się do niego w konkretnych punktach.

Punkt 11 zalecenia w sprawie RFID podkreśla w sposób szczególny, że „*detaliści powinni w punkcie sprzedaży dezaktywować lub usuwać identyfikatory używane w zastosowaniach, chyba że konsumenci […] wyrażą zgodę na dalsze działanie identyfikatorów*”.

W punkcie 12 zezwala się na wyjątek od tej zasady, stwierdzając, że „p*unkt 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*”. Oznacza to, że dezaktywacja w punkcie sprzedaży jest zachowaniem standardowym, o ile ocena skutków w zakresie ochrony danych i prywatności nie stanowi inaczej.

Jednak sekcja D proponowanych ram oceny skutków w zakresie ochrony danych i prywatności oferuje jedynie dwa możliwe wnioski dotyczące sprawozdania z tej oceny: zastosowanie RFID jest albo *„gotowe do wprowadzenia”* albo*„nie jest gotowe do wprowadzenia”*, bez zapewnienia jakiejkolwiek możliwości, aby operator RFID sformułował wniosek w odniesieniu do użycia identyfikatora poza punktem sprzedaży w zastosowaniach detalicznych, zgodnie z wymogiem zawartym w zaleceniu w sprawie RFID. Grupa robocza zauważa, że niektóre zastosowania mogą usprawiedliwiać bądź wymagać, ze szczególnych względów, aby identyfikatory działały nadal poza punktem sprzedaży w sektorze detalicznym. Jednak brak podjęcia takich rozważań w proponowanych ramach wydaje się sugerować, że wszystkie identyfikatory będą dezaktywowane w punkcie sprzedaży.

Ujmując to bardziej ogólnie, grupa robocza zauważa, że podwójne rozwiązanie zaoferowane w sekcji D ram oceny skutków w zakresie ochrony danych i prywatności wydaje się niepotrzebnie restrykcyjne wobec operatorów RFID oraz sektora RFID jako całości. Niektóre zastosowania można uznać za „gotowe do wprowadzenia pod pewnymi warunkami”, które należałoby wymienić we wnioskach sprawozdania z oceny skutków w zakresie ochrony danych i prywatności.

[15] W sekcji 2.3.4. proponowanych ram.

Grupa robocza zachęca autorów proponowanych ram do wyjaśnienia kwestii dezaktywacji identyfikatorów w sektorze detalicznym. Proponowane ramy muszą wyraźnie wymagać, aby operator RFID odniósł się do punktu 12 zalecenia w sprawie RFID do sprawozdania z oceny skutków w zakresie ochrony danych i prywatności, które zostanie opracowane (w przypadku zastosowań sektora detalicznego). **W bardziej ogólnym ujęciu zmienione podejście w zakresie oceny ryzyka powinno zapewnić właściwe narzędzia, aby wyciągnąć wnioski co do warunków lub wprowadzenia zastosowania RFID.**

2.4 Uwagi dodatkowe

Jak podkreślono powyżej w sekcji 2.2, jeśli identyfikator nosi osoba (Użytkownik albo Osoba fizyczna) i jeśli identyfikator zawiera niepowtarzalne dane identyfikacyjne[16], wtedy z definicji identyfikator zawiera dane osobowe. Ściśle rzecz biorąc, definicje „zastosowań poziomu 1" i „zastosowań poziomu 0" przedstawione w sekcji 1.5 są więc sprzeczne: w przypadku większości scenariuszy nie jest możliwe stwierdzenie, że zastosowanie RFID *nie* przetwarza danych osobowych, jeśli identyfikatory noszą Osoby fizyczne lub Użytkownicy. Zatem w ramach tych definicji większość zastosowań kwalifikowałaby się jako zastosowania poziomu 2. **Zastosowania poziomu 0 lub poziomu 1 miałyby więc zastosowanie tylko w tych rzadkich przypadkach, gdy identyfikatory byłyby noszone przez osoby, ale nie posiadałyby niepowtarzalnego numeru**.

Grupa robocza przypuszcza, że autorzy ram nie mieli zamiaru nadać zastosowaniom poziomu 0 i poziomu 1 tak ograniczonego zakresu, a ich definicje nie miały objąć zastosowań, które przetwarzają tylko jeden rodzaj danych osobowych, mianowicie niepowtarzalną tożsamość identyfikatora. Wszystkie definicje poziomów można łatwo wyjaśnić w celu uniknięcia jakichkolwiek niejasności. Właściwe zdefiniowanie metody opartej o ocenę ryzyka mogłoby spowodować przeformułowanie również tych definicji.

Grupa robocza zauważa, że ramy odnoszą się do identyfikatorów *„będących w posiadaniu"* Użytkowników lub Osób fizycznych. Takie wyrażenie jest zbyt restrykcyjne i powinno zostać zastąpione przez „noszone", które znacznie precyzyjniej obejmuje scenariusze ryzyka podczas użytkowania.

Grupa robocza uważa, że proces oceny skutków w zakresie ochrony danych i prywatności zaproponowany w ramach powinien zawierać etap konsultacji z zainteresowanymi stronami. Obejmuje to konsultacje z zainteresowanymi podmiotami (zespoły, związki, stowarzyszenia itd.), na które zastosowanie RFID może mieć wpływ, oraz wymianę opinii, sugestii i propozycji ulepszenia, które pozwolą na wprowadzenie zastosowania w sposób otwarty i sprzyjający ochronie prywatności, co przyniesie korzyści zarówno operatorowi RFID, jak i Użytkownikom lub Osobom fizycznym, których dotyczy. Taka konsultacja z zainteresowanymi stronami wyraźnie przyczynia się do *„informacji i przejrzystości w odniesieniu do stosowania RFID"*, jak i *„działań podnoszących świadomość"* przewidzianych w zaleceniu w sprawie RFID.

Grupa robocza podkreśla także, że szczególne kategorie danych[17] wymagają specyficznych warunków do przetwarzania w sposób zgodny z prawem i bezpieczny. Ramy powinny zapewnić dokładniejsze wytyczne operatorowi FRID w specyficznych kwestiach związanych z przetwarzaniem szczególnych

[16] Odnosimy się w tym miejscu do „danych identyfikacyjnych identyfikatora" (ang. *tag ID*), aby ująć każdy niepowtarzalny numer identyfikacyjny (lub numer seryjny), do którego można mieć dostęp w identyfikatorze RFID i który pozwala na precyzyjne rozpoznanie identyfikatora RFID w konkretnym kontekście.

[17] Artykuł 8 dyrektywy 95/46/WE.

kategorii danych. Określenie wykorzystania szczególnych kategorii danych powinno również stanowić część każdego procesu oceny ryzyka.

Ramy powinny także zapewnić operatorom RFID wytyczne co do właściwego czasu i warunków do przeprowadzenia oceny skutków w zakresie ochrony danych i prywatności w cyklu rozwojowym produktu RFID, w celu rzeczywistego zachęcenia do „*bezpieczeństwa i poszanowania prywatności od samego początku*" zgodnie ze wskazaniem w zaleceniu.

3 Wnioski

Ze względu na kwestie podkreślone w niniejszej opinii, w szczególności brak jasnego i kompleksowego podejścia do oceny ryzyka w zakresie ochrony danych i prywatności w proponowanych ramach, **grupa robocza nie zatwierdza proponowanego dokumentu w obecnej formie.**

Należy podkreślić, że włączenie właściwego procesu oceny ryzyka może wyraźnie ułatwić odniesienie się do wielu innych kwestii, które zostały poruszone w niniejszej opinii. Jeśli wymaga się, aby operator RFID przeprowadził ocenę ryzyka, z pewnością zidentyfikowałby ryzyko związane z niedozwolonym monitorowaniem identyfikatorów RFID noszonych przez osoby. Ponadto w sektorze detalicznym pomocne byłoby podanie jasnego przykładu, aby pokazać, że niektóre identyfikatory RFID (używane w szczególnych zastosowaniach), które *„działają nadal po opuszczeniu punktu sprzedaży[,] nie stanowią zagrożenia dla prywatności lub ochrony danych osobowych"*.

Grupa robocza jest przekonana, że sektor może zaproponować poprawione ramy w oparciu o uwagi podkreślone w niniejszej opinii i jest skłonna podjąć wszystkie możliwe kroki prowadzące do dalszego ulepszania proponowanych ram i doprowadzenia do szybkiego ich zatwierdzenia.

Sporządzono w Brukseli dnia 13 lipca 2010 r.

W imieniu grupy roboczej
Przewodniczący
Jacob KOHNSTAMM