00678/13/PL
WP205

Opinia 04/2013 w sprawie szablonu oceny skutków w zakresie ochrony danych na potrzeby inteligentnych sieci i inteligentnych systemów pomiarowych, opracowanego przez grupę ekspertów nr 2 w ramach grupy zadaniowej Komisji ds. inteligentnych sieci

przyjęta dnia 22 kwietnia 2013 r.

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

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

uwzględniając art. 29 i 30 tej dyrektywy,

uwzględniając swój regulamin wewnętrzny,

PRZYJMUJE NINIEJSZĄ OPINIĘ:

1 Kontekst

1.1 Wprowadzenie

Informacje podstawowe

W dniu 9 marca 2012 r. Komisja Europejska wydała zalecenie w sprawie przygotowań do rozpowszechnienia inteligentnych systemów pomiarowych („zalecenie Komisji") w celu zapewnienia państwom członkowskim wytycznych w zakresie rozpowszechnienia inteligentnych systemów pomiarowych na rynkach energii elektrycznej i gazu. Zalecenie Komisji ma na celu dostarczenie wytycznych w zakresie aspektów ochrony i bezpieczeństwa danych, metodyki oceny ekonomicznej długoterminowych kosztów i korzyści rozpowszechnienia inteligentnych systemów pomiarowych[1] oraz wspólnych minimalnych wymogów funkcjonalnych dotyczących inteligentnych systemów pomiarowych energii elektrycznej.

W odniesieniu do ochrony danych i bezpieczeństwa w kontekście inteligentnych systemów pomiarowych i inteligentnych sieci zalecenie Komisji zawiera wytyczne dla państw członkowskich w sprawie uwzględniania ochrony danych już w fazie projektowania i domyślnej ochrony danych oraz stosowania niektórych zasad ochrony danych określonych w dyrektywie 95/46/WE[2]. Ponadto Komisja przewiduje w tym zaleceniu, że państwa członkowskie powinny przyjąć i stosować szablon oceny skutków w zakresie ochrony danych, który powinien zostać opracowany przez Komisję i przekazany do zaopiniowania Grupie Roboczej ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych (Grupa Robocza Art. 29) w terminie dwunastu miesięcy od opublikowania tego zalecenia. Państwa

[1] Rozpowszechnienie oraz analiza kosztów i korzyści wymagane są na mocy (i) dyrektywy 2009/72/WE dotyczącej wspólnych zasad rynku wewnętrznego energii elektrycznej (Dz.U. L 211 z 14.8.2009, s. 55) oraz (ii) dyrektywy 2009/73/WE dotyczącej wspólnych zasad rynku wewnętrznego gazu ziemnego (Dz.U. L 211 z 14.8.2009, s. 94). Dyrektywa 2012/27/UE w sprawie efektywności energetycznej (Dz.U. L 315 z 14.11.2012, s. 1) zawiera dodatkowe przepisy w sprawie inteligentnych pomiarów. W odniesieniu do rynku energii elektrycznej w dyrektywie 2009/72/WE przewiduje się, że gdy rozpowszechnienie zostanie ocenione pozytywnie, do 2020 r. co najmniej 80 % konsumentów zostanie wyposażonych w inteligentne systemy pomiarowe. Dla rynku gazu nie podano żadnych dokładnych ram czasowych.

[2] Dyrektywa 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, Dz.U. L 281 z 23.11.1995, s. 31-50.

członkowskie powinny dopilnować, aby operatorzy sieci i operatorzy inteligentnych systemów pomiarowych przedsięwzięli odpowiednie środki techniczne i organizacyjne w celu zapewnienia ochrony danych osobowych zgodnie z szablonem oceny skutków w zakresie ochrony danych, uwzględniając opinię Grupy Roboczej Art. 29 na temat tego szablonu[3].

Komisja ponadto przewiduje w zaleceniu, że szablon oceny skutków w zakresie ochrony danych powinien obejmować „opis przewidywanych operacji przetwarzania, ocenę zagrożeń dla praw i wolności osób, których dotyczą dane, środki przewidziane w celu sprostania zagrożeniom, zabezpieczenia, środki i mechanizmy bezpieczeństwa mające zagwarantować ochronę danych osobowych oraz wykazać zgodność z przepisami dyrektywy 95/46/WE, uwzględniając prawa i słuszne interesy osób, których dotyczą dane, i zainteresowanych osób".

Przygotowania

W lutym 2012 r. Komisja przedłużyła mandat grupy ekspertów nr 2 („EG2") w ramach swojej grupy zadaniowej ds. inteligentnych sieci („SGTF"), aby grupa ta opracowała szablon oceny skutków w zakresie ochrony danych na potrzeby inteligentnych sieci. Grupa ekspertów nr 2, która składa się głównie z przedstawicieli branży, zorganizowała cztery warsztaty w 2012 r. W warsztatach tych udział wzięły CNIL[4], EIOD[5] i ICO[6] w charakterze obserwatorów w imieniu Grupy Roboczej Art. 29.

W dniu 26 października 2012 r. Grupa Robocza Art. 29 wysłała pismo do Dyrekcji Generalnej ds. Energii Komisji Europejskiej („DG ENER") w celu zwrócenia uwagi Komisji na kilka aspektów projektu szablonu oceny skutków w zakresie ochrony danych, które to aspekty zdaniem Grupy Roboczej Art. 29 wymagały znacznych ulepszeń. Między innymi pismo to zawierało zalecenie, że w szablonie oceny skutków w zakresie ochrony danych należy:

(i) jasno określić podmioty i ich obowiązki,
(ii) skupić się na czynnikach ryzyka dla ochrony danych i prywatności zainteresowanych osób fizycznych,
(iii) zawrzeć lepsze wskazówki dla podmiotów pod względem dopasowania odpowiednich kontroli do każdego czynnika ryzyka, oraz
(iv) zaoferować bardziej szczegółowe i praktyczne wytyczne odnośnie do sposobu uwzględnienia ryzyka dla ochrony danych i prywatności w kontekście inteligentnych sieci.

Uwagi te poczyniono bez uszczerbku dla ostatecznej oceny szablonu oceny skutków w zakresie ochrony danych dokonywanej przez Grupę Roboczą Art. 29.

---

[3] EG2 jako punkt wyjścia wykorzystała doświadczenia w zakresie opracowania i zmiany, w oparciu o uwagi Grupy Roboczej Art. 29 („GR29"), „Propozycji sektora w sprawie ram oceny skutków w zakresie ochrony danych i prywatności w zastosowaniach RFID".

[4] La Commission Nationale de l'Informatique et des Libertés, francuski krajowy organ nadzoru ds. ochrony danych osobowych.

[5] Europejski Inspektor Ochrony Danych, organ nadzoru ds. ochrony danych osobowych przez instytucje i organy unijne.

[6] Information Commissioner's Office, krajowy organ nadzoru ds. ochrony danych osobowych w Zjednoczonym Królestwie.

Szablon oceny skutków w zakresie ochrony danych

W dniu 8 stycznia 2013 r. Komisja przedłożyła Grupie Roboczej Art. 29 ostateczną wersję szablonu oceny skutków w zakresie ochrony danych przygotowanego przez zainteresowane strony z EG2. W piśmie towarzyszącym szablonowi oceny skutków w zakresie ochrony danych Komisja zauważyła, że może rozważyć przyjęcie szablonu oceny skutków w zakresie ochrony danych przygotowanego przez zainteresowane strony z EG2 w formie zalecenia Komisji z zastrzeżeniem uwag Grupy Roboczej Art. 29 i ich odpowiedniego uwzględnienia[7].
Niniejsza opinia zawiera uwagi na temat proponowanego szablonu oceny skutków w zakresie ochrony danych.

Struktura niniejszej opinii

W sekcji 1.2 podkreślono znaczenie ochrony prywatności i danych dla pomyślnego wdrożenia inteligentnych sieci. W sekcji 1.3 opisano cele procesu oceny skutków w zakresie ochrony danych. Sekcja 2 zawiera ocenę szablonu oceny skutków w zakresie ochrony danych dokonaną przez Grupę Roboczą Art. 29. W sekcji 3 wyciągnięto ostateczne wnioski. Sekcję 2 uzupełniono załącznikiem I, w którym przedstawiono bardziej szczegółowe uwagi i sugestie.

1.2 Inteligentne sieci i ochrona danych

Grupa Robocza Art. 29 przypomina swoją poprzednią opinię WP183 w sprawie inteligentnych pomiarów[8], a także opinię Europejskiego Inspektora Ochrony Danych („EIOD") z dnia 8 czerwca 2012 r. na temat zalecenia Komisji[9].

W obu tych opiniach podkreśla się znaczenie ochrony danych w kontekście inteligentnych sieci i inteligentnych pomiarów oraz przedstawia się wytyczne i zalecenia w zakresie ochrony praw do ochrony danych osobowych w związku z wprowadzeniem inteligentnego pomiaru i inteligentnych sieci w Europie. W niniejszej sekcji kontekst i kluczowe kwestie ochrony danych będą zatem opisane tylko pokrótce.

Inteligentne systemy pomiarowe i inteligentne sieci mają na celu umożliwienie produkcji, dystrybucji i wykorzystywania energii w sposób inteligentny i zracjonalizowany.

Kluczową cechą inteligentnych liczników energii elektrycznej i gazu jest to, że mogą

---

[7] W dniu 17 stycznia 2013 r. szablon oceny skutków w zakresie ochrony danych przedłożono także Radzie Europejskich Regulatorów Energetyki (CEER). Przewodniczący CEER udzielił odpowiedzi w dniu 5 marca, z zadowoleniem przyjmując prace EG2 i będący ich efektem projekt szablonu. Ponownie wspomniał w swoim piśmie o znaczeniu bezpieczeństwa, ochronie danych i potrzebie zachowania przez klientów kontroli nad ich danymi, odniósł się do poprzednich wskazówek CEER opublikowanych w 2011 r. i wezwał do szybkiego działania na rzecz ukończenia prac nad szablonem oceny skutków w zakresie ochrony danych.

[8] Opinia 12/2011 Grupy Roboczej Art. 29 w sprawie inteligentnych pomiarów, przyjęta dnia 4 kwietnia 2011 r. (WP183).

[9] Opinia EIOD jest dostępny na stronie internetowej EIOD pod adresem http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-06-08_Smart_metering_EN.pdf.

one dostarczać danych poprzez zdalną łączność między licznikiem a dostawcami energii, operatorami sieci i innymi osobami trzecimi. Inteligentne liczniki umożliwiają również częstszą komunikację. Za pomocą inteligentnych liczników będzie można bardzo często odczytywać i rejestrować zużycie energii, na przykład co piętnaście minut.

Inteligentne systemy pomiarowe stanowią ważne elementy składowe inteligentnej sieci, która jest inteligentną dwukierunkową siecią elektryczną, w której informacje pochodzące od użytkowników tej sieci są łączone w celu m.in. planowania zaopatrzenia w energię elektryczną w sposób bardziej efektywny i opłacalny.

Upowszechnienie w całej Europie „inteligentnych systemów pomiarowych" umożliwia masowe gromadzenie danych osobowych z europejskich gospodarstw domowych, jak dotąd bezprecedensowe pod względem szczegółowości i kompleksowego zakresu: inteligentny pomiar może umożliwiać śledzenie zachowań osób w ich własnych domach, a tym samym tworzenie szczegółowych profili wszystkich osób na podstawie ich aktywności w domach.

Ze szczegółowych danych dotyczących zużycia energii, zebranych przez inteligentne liczniki, można uzyskać wiele informacji na temat korzystania przez konsumentów z określonych towarów lub urządzeń, codziennych zajęć, warunków życia, działań, stylu życia i zachowania[10].

Zastosowanie inteligentnych sieci i inteligentnych systemów pomiarowych stwarza tym samym nowe czynniki ryzyka dla osób, których dane dotyczą, mające potencjalny wpływ w różnych obszarach (np. w zakresie dyskryminacji cenowej, profilowania reklamy behawioralnej, podatków, dostępu na potrzeby ochrony porządku publicznego, bezpieczeństwa domowego), które to czynniki ryzyka wcześniej nie były powiązane z sektorem energetyki, a były bardziej typowe i już obecne tylko w innych środowiskach (w telekomunikacji, handlu elektronicznym i Web 2.0).

Inteligentny pomiar to również jedna z pierwszych rozpowszechnionych aplikacji, które zwiastują przyszłość „internetu przedmiotów". Czynniki ryzyka, jakie stanowią zbieranie i dostępność szczegółowych danych dotyczących zużycia energii, mogą w przyszłości wzrosnąć, biorąc pod uwagę coraz większą dostępność danych z innych źródeł, takich jak: dane określające położenie geograficzne, dane dostępne poprzez śledzenie i profilowanie w internecie, systemy nadzoru wideo i systemy identyfikacji radiowej (RFID), z którymi dane z inteligentnych pomiarów mogą być łączone[11].

[10] Można to zilustrować następującym przykładem: wykazano, że przy odczycie co 2 sekundy możliwe jest nawet określenie, jakie treści multimedialne są wykorzystywane w danym gospodarstwie domowym: http://www.its.fh-muenster.de/greveler/pubs/preprint_online.pdf.

[11] Rekomendacja Komitetu Ministrów Rady Europy CM/Rec(2010)13 z dnia 23 listopada 2010 r. dla państw członkowskich w sprawie ochrony osób fizycznych w związku z automatycznym przetwarzaniem danych osobowych w kontekście tworzenia profili.

1.3 Cele szablonu oceny skutków w zakresie ochrony danych

Poprzez swoje zalecenie Komisja Europejska chce zachęcić administratorów danych do przeprowadzania oceny skutków w zakresie ochrony danych w celu osiągnięcia następujących korzyści:

- w ocenie skutków w zakresie ochrony danych należy ująć opis przewidywanych operacji przetwarzania, ocenę ryzyka dla praw i wolności osób, których dotyczą dane, środki przewidziane w celu sprostania czynnikom ryzyka, zabezpieczenia, środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych oraz wykazać zgodność z przepisami dyrektywy 95/46/WE;

- ocena skutków w zakresie ochrony danych powinna być również pomocna krajowym organom ochrony danych w ocenie zgodności przetwarzania oraz, w szczególności, czynników ryzyka dla ochrony danych osobowych osoby, której dotyczą dane, i związanych z nimi zabezpieczeń, gdy administratorzy danych zasięgają ich opinii przed rozpoczęciem przetwarzania danych, zgodnie z zaleceniem Komisji[12]. Ocena skutków w zakresie ochrony danych powinna zatem również pomagać administratorowi danych w wykazaniu zgodności z dyrektywą 95/46/WE[13].

Ponadto ocena skutków w zakresie ochrony danych może pomóc konsumentom, administratorom danych, organom ochrony danych, organom regulacji energetyki, organizacjom ochrony konsumentów i innym zainteresowanym stronom w uzyskaniu lepszego wglądu w określone aspekty ochrony danych w aplikacjach inteligentnych pomiarów i inteligentnych sieci. Informacje pochodzące z oceny skutków w zakresie ochrony danych mogą również pomagać organom ochrony danych w zidentyfikowaniu zarówno najlepszych praktyk, jak i ewentualnych docelowych obszarów wysokiego ryzyka na potrzeby kontroli.

W państwach członkowskich, w których zastosowanie aplikacji inteligentnych pomiarów i inteligentnych sieci wymaga wcześniejszego powiadomienia / kontroli wstępnej, ocena skutków w zakresie ochrony danych może uprościć ten proces zarówno dla organów ochrony danych, jak i dla administratorów danych. Ocena skutków w zakresie ochrony danych powinna zatem również pomagać administratorowi danych w wykazaniu zgodności z dyrektywą 95/46/WE.

Należy wreszcie podkreślić, że proponowane rozporządzenie o ochronie danych[14] zwiększyłoby znaczenie procesu oceny skutków w zakresie ochrony danych, która

[12] Rekomendacja ta pozostaje bez uszczerbku dla prawnego obowiązku przeprowadzania kontroli wstępnej w państwach członkowskich, w zależności od cech operacji przetwarzania.

[13] Dyrektywa 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, Dz.U. L 281 z 23.11.1995, s. 31.

[14] W dniu 25 stycznia 2012 r. Komisja przyjęła pakiet na potrzeby reformy europejskich ram ochrony danych. Pakiet ten obejmuje (i) „komunikat" (COM(2012) 9 wersja ostateczna), (ii) „proponowane

jest uważana za kluczowe narzędzie pomagające zapewnić odpowiedzialność administratorów danych.

1.4 Krótki opis proponowanego szablonu oceny skutków w zakresie ochrony danych

EG2 wyjaśnia, że jako punkt wyjścia w swojej pracy wykorzystała doświadczenia w zakresie opracowania i zmiany, w oparciu o uwagi Grupy Roboczej Art. 29 („GR29"), „Propozycji sektora w sprawie ram oceny skutków w zakresie ochrony danych i prywatności w zastosowaniach RFID".

W szablonie oceny skutków w zakresie ochrony danych zaproponowanym przez EG 2 najpierw wyjaśnione są cel i zakres procesu, płynące z niego korzyści oraz zainteresowane strony. Następnie omówione jest podejście pozwalające na przeprowadzenie oceny skutków w zakresie ochrony danych w ośmiu etapach i podane są punkt po punkcie wytyczne dla administratora danych dotyczące sposobu przeprowadzania tej oceny.

2 Analiza szablonu oceny skutków w zakresie ochrony danych

Grupa Robocza Art. 29 dziękuje zainteresowanym stronom z EG2 za przeprowadzenie szeroko zakrojonych prac i z zadowoleniem przyjmuje główne cele tych prac podkreślone we wprowadzających sekcjach szablonu oceny skutków w zakresie ochrony danych.

Chociaż zasadniczo przedstawione w zaproponowanym dokumencie podejście oparte na ośmiu etapach jest rzetelne, to Grupa Robocza Art. 29 zidentyfikowała kilka krytycznych problemów związanych z metodyką, a także z treścią samego szablonu oceny skutków w zakresie ochrony danych. Problemy te szczegółowo opisano w poniższych sekcjach.

2.1 Brak przejrzystości co do charakteru i celów oceny skutków w zakresie ochrony danych

Zgodnie z definicją zawartą w sekcji 3 lit c) zalecenia Komisji ocena skutków w zakresie ochrony danych „oznacza uporządkowany proces oceny ewentualnych skutków zagrożeń, w przypadku gdy operacje przetwarzania mogą powodować określone zagrożenia dla praw i wolności osób, których dotyczą dane, ze względu na ich charakter, zakres lub cel", przeprowadzany przez administratora danych lub przetwarzającego działającego w imieniu administratora.

Grupa Robocza Art. 29 zgadza się z tą definicją i dlatego celem oceny skutków w zakresie ochrony danych powinna być ocena skutków czynników ryzyka dla osób, których dane dotyczą.

Grupa Robocza Art. 29 ubolewa jednak, że przedłożony szablon oceny skutków w zakresie ochrony danych nie uwzględnia bezpośrednio faktycznych skutków dla osób,

---

rozporządzenie o ochronie danych" (COM(2012) 11 wersja ostateczna) oraz (iii) „proponowaną dyrektywę o ochronie danych" (COM(2012) 10 wersja ostateczna).

których dane dotyczą, na przykład strat finansowych wynikających z niedokładnego wystawiania faktur, dyskryminacji cenowej lub przestępstw ułatwionych przez nieupoważnione profilowanie. Nawet jeżeli cele w zakresie ochrony danych i prywatności wymienione w załączniku I mogą być bardzo przydatne dla ułatwienia uzyskania zgodności, to są one niewystarczające w kontekście podejścia opierającego się na analizie ryzyka. Ocena potencjalnych skutków dla osób, których dane dotyczą, jest niezbędnym elementem takiego podejścia.

Dlatego Grupa Robocza Art. 29 uważa, że szablon oceny skutków w zakresie ochrony danych w swojej obecnej formie nie może osiągnąć celu określonego w zaleceniu Komisji. Ocena skutków w zakresie ochrony danych nie zapewnia praktycznego narzędzia na potrzeby oceny skutków dla osób, których dane dotyczą.

Jeżeli czynniki ryzyka i ich skutki dla osób, których dane dotyczą, nie zostaną uwzględnione w całości, niemożliwe jest poprawne określenie i wdrożenie niezbędnych środków kontroli i zabezpieczeń.

2.2 Błędy metodologiczne w szablonie oceny skutków w zakresie ochrony danych

Grupa Robocza Art. 29 uważa, że poza wyżej określonym kluczowym niedociągnięciem, a czasami w powiązaniu z nim, szablon oceny skutków w zakresie ochrony danych zawiera kilka błędów metodologicznych, które zagrażają jego stosowaniu.

Po pierwsze, w zaproponowanym szablonie oceny skutków w zakresie ochrony danych często myli się czynniki ryzyka z zagrożeniami[15].

Po drugie, czynniki ryzyka, które należy ograniczyć, nie są dopasowane do wykazu możliwych środków kontroli zawartego w załączniku II. Nawet jeżeli każdy scenariusz dotyczący ryzyka jest specyficzny i powinien być oceniany pod względem jego cech szczególnych, to często możliwe jest zidentyfikowanie pewnych kategorii środków kontroli jako skutecznych w ograniczaniu określonych kategorii ryzyka. Typowym tego przykładem jest norma bezpieczeństwa informacji ISO/IEC 27002:2005, w której środki kontroli przedstawiono jako najlepsze praktyki służące ograniczaniu czynników ryzyka w określonych obszarach. Chociaż zaproponowane środki ograniczające ryzyko nie zastępują potrzeby wprowadzenia procesu opierającego się na analizie ryzyka, mogą stanowić punkt odniesienia dla skutecznego i spójnego podejścia. Na przykład ryzyko związane z przechwytywaniem w

[15] Zob. definicja ryzyka w zakresie bezpieczeństwa informacji w ISO/IEC 27005:2008 – „możliwość, że dane zagrożenie będzie wykorzystywało słabe strony składnika aktywów lub grupy aktywów i powodowało w ten sposób szkody dla organizacji". Nie ma bezpośredniej definicji zagrożeń, lecz można opracować ich definicję operacyjną na podstawie ISO/IEC 27001:2005. Zagrożenia zatem odnoszą się do możliwości wykorzystania słabych stron w aktywach, które mają być chronione. Będzie to miało następnie skutki dla tych aktywów w postaci utraty cech bezpieczeństwa. Przykład typowych zagrożeń związanych z bezpieczeństwem są wymienione w załączniku C do ISO/IEC 27005:2008.
Zob. również metodyka CNIL: http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf oraz sprawozdanie ENISA „Krajobraz zagrożeń": https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape/at_download/fullReport).

niezabezpieczonym kanale danych dotyczących zużycia energii można na ogół ograniczyć poprzez techniki szyfrowania. Szczegółowa ocena ryzyka może następnie prowadzić do wyboru określonych algorytmów szyfrowania i długości klucza bądź innych lub uzupełniających środków ograniczania ryzyka, a nawet do akceptacji ryzyka lub przeniesienia ryzyka (a tym samym braku środków ograniczania ryzyka).

Ponadto zaproponowany szablon oceny skutków w zakresie ochrony danych nie zawiera również wystarczająco szczegółowych i dokładnych wytycznych odnośnie do pojęcia podatności, sposobu obliczania ryzyka i szeregowania go pod względem ważności, wyboru odpowiednich środków kontroli i oceny ryzyka szczątkowego, które pozostaje po wprowadzeniu środków kontroli. Mimo że szablon oceny skutków w zakresie ochrony danych zawiera odniesienie do dokumentu zewnętrznego, Grupa Robocza Art. 29 wolałaby, żeby w szablonie znajdowało się więcej wytycznych i wyjaśnień dotyczących samego szablonu, tak aby dostarczyć czytelnikowi niezależny dokument. Nie jest też oczywiste, w jaki sposób należy wypełniać zaproponowane formularze.

W końcu szablon oceny skutków w zakresie ochrony danych nie zapewnia wystarczających wskazówek co do określania roli i obowiązków różnych zainteresowanych stron w odniesieniu do ochrony danych. Jedynym odwołaniem jest odniesienie do innego dokumentu EG2. Przyszłe aplikacje inteligentnych sieci będą zróżnicowane i oferowane przez wiele zainteresowanych stron. Wydaje się zatem, że decydujące znaczenie ma zapewnienie branży wytycznych umożliwiających określenie administratorów danych i przetwarzających dane. Na przykład szablon oceny skutków w zakresie ochrony danych mógłby zawierać w ramach trzeciego etapu czwartą sekcję, która dotyczyłaby określania różnych obowiązków podmiotów zaangażowanych w przetwarzanie danych.

Dalsze szczegółowe informacje na temat tych i innych niedociągnięć metodologicznych przedstawiono w załączniku 1.

2.3 W szablonie oceny skutków w zakresie ochrony danych brakuje treści odnoszących się do danego sektora: należy zidentyfikować i dopasować czynniki ryzyka charakterystyczne dla tej branży oraz stosowne środki kontroli służące ograniczeniu tych czynników ryzyka

W szablonie oceny skutków w zakresie ochrony danych brakuje treści odnoszących się do danego sektora. Zarówno czynniki ryzyka, jak i środki kontroli wymienione w szablonie mają charakter ogólny i tylko w niektórych miejscach szablon zawiera wytyczne dotyczące przedmiotowej branży - najlepsze praktyki, które mogłyby być rzeczywiście przydatne. Krótko mówiąc, czynniki ryzyka i środki kontroli nie odzwierciedlają doświadczeń branży odnośnie do najważniejszych obaw i najlepszych praktyk.

Grupa Robocza Art. 29 rozumie, że EG2 obecnie pracuje nad zebraniem „najlepszych dostępnych technik” („BAT”), które umożliwiłyby organizacji przeprowadzającej ocenę skutków w zakresie ochrony danych wybranie odpowiednich środków w razie konieczności, co tym samym stanowiłoby odpowiedź na część uwag krytycznych zawartych w poprzedniej sekcji. Grupa Robocza Art. 29 podkreśla znaczenie tego

dokumentu, który stanowi uzupełnienie szablonu oceny skutków w zakresie ochrony danych.

Dokument zawierający najlepsze dostępne techniki nie może jednak zastępować określenia w samym szablonie oceny skutków w zakresie ochrony danych najpowszechniejszych czynników ryzyka charakterystycznych dla tej branży i możliwych środków kontroli tych czynników ryzyka. Jest to tym bardziej istotne, że - w przeciwieństwie do tego szablonu oceny skutków w zakresie ochrony danych - dokument zawierający najlepsze dostępne techniki nie zostanie przekazany Grupie Roboczej Art. 29 w celu ocenienia go i udzielenia wskazówek, nie jest też planowane przyjęcie tego dokumentu przez Komisję. Biorąc pod uwagę zidentyfikowane niedociągnięcia w szablonie oceny skutków w zakresie ochrony danych, Komisja powinna rozważyć włączenie do niego najlepszych dostępnych technik i przedłożenie połączonego dokumentu Grupie Roboczej Art. 29 do zaopiniowania.

Ponadto koncepcja szablonu oceny skutków w zakresie ochrony danych różni się od koncepcji ram takiej oceny. W ramach należy określić cele, przedstawić metodykę i ustalić zakres oceny pod względem granic analizowanego systemu/procesu. Szablon powinien być bardziej rozwinięty – powinien zapewniać operacyjny instrument zarządzania czynnikami ryzyka związanymi z określonym systemem/procesem oraz przypadkami wykorzystywania tego systemu/procesu, wskazywać możliwe środki kontroli oraz najlepsze dostępne techniki ograniczania tych czynników ryzyka, a także dostarczać szczegółowych wytycznych. Jest to szczególnie potrzebne w przypadkach, gdy niedostępna jest konkretna wiedza ekspercka (na przykład w MŚP lub - w przypadku inteligentnych sieci – w sektorze przemysłu, który wcześniej nie miał wiele styczności z kwestiami ochrony prywatności i danych).

Celem szablonu oceny skutków w zakresie ochrony danych powinno być opracowanie wytycznych w większym stopniu związanych z daną branżą i łatwiejszych do zastosowania. W szczególności konieczne jest lepsze zdefiniowanie potencjonalnych skutków dla osób, których dane dotyczą, w kontekście inteligentnych sieci i zapewnienie bardziej precyzyjnych wytycznych co do rodzaju środków kontroli, które można wdrożyć.

Komisja mogła zapewnić EG2 ogólną metodykę oceny ryzyka dla prywatności i ochrony danych[16]. Z kolei EG2 mogła zastosować taką metodykę i w oparciu o nią opracować szablon oceny skutków w zakresie ochrony danych bardziej dostosowany do branży. Podejście to umożliwiłoby EG2 skupienie się na istotnych kwestiach, takich jak czynniki ryzyka i środki kontroli charakterystyczne dla inteligentnych sieci, i jednoczesne oparcie się na ramach odniesienia pod względem podstawowych aspektów metodologicznych. Grupa Robocza Art. 29 sugeruje, aby EG2 i Komisja przyjęły to podejście na potrzeby przyszłych prac nad tym szablonem oceny skutków w zakresie ochrony danych i wszelkich innych sektorowych szablonów oceny.

3 Wnioski i zalecenia

Grupa Robocza Art. 29 dostrzega postępy poczynione w stosunku do wcześniejszych wersji oraz przydatne elementy, które szablon oceny skutków w zakresie ochrony

[16] Zob. np. wyżej wspomniana metodyka CNIL.

danych już zawiera. Jest jednak zdania, że szablon oceny skutków w zakresie ochrony danych w swojej obecnej formie nie jest wystarczająco dojrzały i dopracowany.

Grupa Robocza Art. 29 zaleca zatem, aby Komisja podjęła niezbędne kroki w celu zapewnienia kontynuacji prac nad szablonem oceny skutków w zakresie ochrony danych oraz zagwarantowania, że produkt końcowy zapewni administratorom danych wystarczająco szczegółowe, użyteczne i jasne praktyczne wytyczne.

Aby ułatwić przyszłe prace, Grupa Robocza Art. 29 zawarła w załączniku 1 do niniejszej opinii pewne bardziej szczegółowe zalecenia. Ze względu na wady metodologiczne dokumentu i jego brak specyfiki dla kontekstu inteligentnych sieci Grupa Robocza Art. 29 nie jest jednak w stanie przedstawić na tym etapie dalszych, bardziej szczegółowych i jednoznacznych uwag.

Biorąc pod uwagę zidentyfikowane niedociągnięcia w szablonie oceny skutków w zakresie ochrony danych, Grupa Robocza Art. 29 zaleca Komisja, aby rozważyła włączenie do niego najlepszych dostępnych technik i przedłożenie połączonego dokumentu Grupie Roboczej Art. 29 do zaopiniowania[17].

Ponadto Grupa Robocza Art. 29 zaleca Komisji - w szerszym kontekście – aby zrobiła bilans wcześniejszych i obecnych prac w dziedzinie oceny skutków w zakresie ochrony danych[18] i rozważyła możliwość określenia ogólnej metodyki dokonywania takiej oceny, która mogłaby być przydatna w pracach związanych z określonym obszarem.

Wreszcie w odniesieniu do konieczności przeprowadzania obowiązkowej oceny skutków Grupa Robocza Art. 29 przywołuje doświadczenia uzyskane w ramach oceny skutków w zakresie ochrony danych w odniesieniu do RFID i podkreśla, że dostępne w państwach członkowskich dane statystyczne wskazują na to, iż oceny skutków dotyczące RFID zostały wykorzystane w wyjątkowo niskim stopniu. Podczas gdy statystyki te mogą wynikać z kilku podstawowych przyczyn, to jednym z najważniejszych czynników, który przyczynił się do takiego stanu rzeczy, zdecydowanie wydaje się obecny brak obowiązku przeprowadzania takiej oceny skutków.

Sporządzono w Brukseli dnia 22 kwietnia 2013 r.

W imieniu Grupy Roboczej
Przewodniczący
Jacob KOHNSTAMM

[17] Nie wyklucza to możliwości okresowego aktualizowania w przyszłości dokumentu zawierającego BAT w celu uwzględnienia zmian technologicznych i stanu techniki.

[18] Zob. np. projekt PIAF: http://www.piafproject.eu/Index.html, jak również istniejącą metodykę, którą wspomniano wcześniej.

Załącznik 1: Szczegółowe uwagi na temat szablonu oceny skutków w zakresie ochrony danych

Niniejszy załącznik stanowi uzupełnienie sekcji 2 opinii. Struktura uwag odpowiada strukturze szablonu oceny skutków w zakresie ochrony danych.

→ Zakres oceny skutków w zakresie ochrony danych

- Szablon nie zawiera precyzyjnej definicji i opisu typów operacji przetwarzania danych, które są przedmiotem oceny skutków w zakresie ochrony danych. Ponadto zakres tej oceny nie jest dokładnie określony w sekcji 1.2 szablonu. W zaleceniu Komisji jasno zdefiniowano ocenę skutków w zakresie ochrony danych jako „uporządkowany proces oceny ewentualnych skutków zagrożeń, w przypadku gdy operacje przetwarzania mogą powodować określone zagrożenia dla praw i wolności osób, których dotyczą dane, ze względu na ich charakter, zakres lub cel". Definicja ta obejmuje prawa podstawowe określone w art. 7 i 8 Karty praw podstawowych Unii Europejskiej („Karta"), odpowiednio prawo do prywatności i prawo do ochrony danych osobowych. Należy wziąć pod uwagę fakt, że szablon jest związany z ochroną danych osobowych określoną w dyrektywie 95/46/WE[19].
- Jak podkreślono w uwagach ogólnych, szablon oceny skutków w zakresie ochrony danych powinien odnosić się przede wszystkim do skutków dla osoby, której dane dotyczą. Podczas gdy trzeba zrealizować określone w załączniku I cele w zakresie ochrony prywatności i danych oraz osiągnąć zgodność z przepisami o ochronie danych, zgodność z tymi przepisami nie jest celem samym w sobie i dla siebie samego. Ostatecznym celem procesu oceny skutków w zakresie ochrony danych jest zatem określenie środków kontroli minimalizujących wszelki niekorzystny wpływ na prawa i wolności osób, których dane dotyczą.
- Poniższe przykłady mogą pomóc zilustrować różnicę między podejściem zredukowanym tylko do kontroli zgodności a podejściem opartym na ocenie realnego ryzyka mającego analogiczny realny wpływ na osoby, których dane dotyczą.
    - Ryzyko związane z przestępczością: jeśli techniczne i organizacyjne środki podjęte w celu zapewnienia bezpieczeństwa danych dotyczących zużycia energii są niewystarczające, dostęp do takich danych w odniesieniu do pojedynczego gospodarstwa domowego może zostać uzyskany bezprawnie. Może to zwiększyć ryzyko, że dany konsument padnie ofiarą przestępstwa. Na przykład znajomość wzoru zachowań, którą można uzyskać na podstawie danych dotyczących zużycia energii, a konkretnie wiedza, że dom jest pusty w określonym czasie, może prowadzić do zwiększonego ryzyka włamań i kradzieży.

[19] Wszelkie odesłania do pojęcia „prywatności danych" lub próby podania w sekcji 1.2 lub glosariuszu definicji *ad hoc* „prywatności" są zbędne i mogłyby wprowadzać w błąd. Tam, gdzie to możliwe, należy stosować terminologię dyrektywy 95/46/WE. Artykuły 7 i 8 Karty można przytoczyć i odwoływać się do nich na potrzeby uzyskania dalszych wytycznych.

- Jeżeli dane dotyczące zużycia energii zostaną sfałszowane, konsumenci mogą otrzymać błędnie wystawione rachunki[20].
- Profilowanie, wykluczenie, dyskryminacja, niezamówione informacje handlowe: większa dostępność danych dotyczących konsumentów objętych inteligentnymi sieciami może prowadzić do nasilenia profilowania, co z kolei może prowadzić do dyskryminacji cenowej i wykluczenia (np. wpisywanie na czarną listę, wyższe taryfy), stosowania niezamówionych ukierunkowanych reklam behawioralnych, jak również do ogólnego braku równowagi w sytuacji ekonomicznej konsumenta względem usługodawców/administratorów danych, co następnie może być wykorzystywane w niewłaściwy sposób.
- Ryzyko niezgodnego z określonymi celami i bezprawnego wykorzystywania danych przez organy ścigania lub inne osoby trzecie, ryzyko nasilonego nadzoru ze strony władz (które można byłoby zmniejszyć na przykład poprzez ograniczenie przetwarzanych danych osobowych do minimum).

- Powyższe i inne przykłady czynników ryzyka i możliwych skutków dla osób, których dane dotyczą, powinny być uwzględnione i ujęte w ocenie skutków.

→Zainteresowane strony

- W szablonie oceny skutków w zakresie ochrony danych nie bierze się pod uwagę roli i funkcji różnych podmiotów w ekosystemie inteligentnych sieci, a zatem nie rozróżnia się ich obowiązków. Inteligentne sieci mogą jednak zrealizować swoje cele wyłącznie przy zorganizowanej współpracy różnych organizacji w nich uczestniczących i wymianie danych pomiędzy nimi. Aby opracować konstruktywną ocenę skutków w zakresie ochrony danych, uczestnicy będą musieli współpracować. Proponowany szablon oceny skutków w zakresie ochrony danych nie zawiera wystarczających wskazówek co do sposobu przeprowadzania tej oceny, w przypadku gdy ma ona dotyczyć kilku operatorów, którzy wykonują powiązane czynności przetwarzania danych.
- Zastosowany w sekcji 1.3.3. termin „operator inteligentnej sieci" jest określeniem o charakterze bardzo ogólnym i nie uwzględnia faktu, że różne podmioty mogą wykonywać różne funkcje w krajobrazie inteligentnych sieci, co silnie wpływa na granice i zakres przeprowadzanej oceny skutków w zakresie ochrony danych[21]. Funkcje te powinny być opisane ze szczególnym naciskiem na ich rolę w wymianie danych osobowych niezbędnych do przeprowadzania procesów biznesowych inteligentnych sieci. Szablon oceny skutków w zakresie ochrony danych powinien zawierać zwięzłe i aktualne określenie ról stron zaangażowanych w proces tej oceny (zob. np. sprawozdanie EG2 z dnia 16 lutego 2011 r.[22]).

---

[20] W odniesieniu do wystawiania faktur podobne ryzyko może również dotyczyć właścicieli paneli fotowoltaicznych lub małych elektrowni kogeneracyjnych.

[21] Zob. np. http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/SGConceptualModel#Smart_Grid_Conceptual_Model_Doma.

[22] Zob. http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2.pdf.

- Należy dodać przypomnienie o konieczności przestrzegania obowiązującego ustawodawstwa.
- W szablonie oceny skutków w zakresie ochrony danych należy również wymienić jako zainteresowane strony (i) odbiorców danych oraz (ii) (ewentualnych) inspektorów ochrony danych danej organizacji.

→ Etap 1

- Konieczne jest ponowne rozpatrzenie kryteriów oceny wstępnej. W związku z tym trzeba dokonać również przeglądu kwestionariusza w sekcji 3.1. Jest to konieczne także dla zapewnienia zgodności z sekcją 2.1.
- Należy zmienić kolejność kryteriów, aby odzwierciedlała logiczną kolejność, w jakiej powinny być rozpatrywane:
    1. Czy dane osobowe są przetwarzane?
    2. Czy organizacja jest administratorem danych?
    3. Czy przetwarzanie danych wywołuje jakiekolwiek skutki dla praw i wolności?
    4. Kiedy nastąpi odpowiedni czas i jaka będzie motywacja?
- Wśród rodzajów danych, które w szablonie oceny skutków w zakresie ochrony danych są wymienione jako takie, które można uznać za dane osobowe, niektóre wyraźnie nie stanowią danych osobowych (prognoza zapotrzebowania budynku, kampusu i organizacji), natomiast niektóre dane, które mogą być danymi osobowymi, nie są wymienione lub są wymienione błędnie (temperatura wewnątrz domu może stanowić dane osobowe, ponieważ może wskazywać na to, czy dom jest zamieszkany; kolejne miejsca, w których ładowano samochód elektryczny, są danymi osobowymi, ponieważ wskazują na lokalizację użytkownika itd.). Należy zapewnić obszerniejsze wytyczne, aby pomóc organizacji zidentyfikować dane osobowe, które będą przetwarzane.
- Ponadto - również w kontekście kryterium 1 - ocena skutków w zakresie ochrony danych powinna być dokonywana także w odniesieniu do istniejących systemów, które nie zostały utworzone z uwzględniania ochrony danych już w fazie projektowania i w przypadku których wcześniej nie przeprowadzono żadnej oceny skutków. Powinno to być zaznaczone w tekście, na przykład w dodatkowym punkcie w wykazie elementów powodujących konieczność przeprowadzenia oceny skutków, który już opracowano w dziale „Odpowiedni czas", lub w osobnym akapicie po tym wypunktowaniu.

→ Etap 2

- Ważne jest zapewnienie - jeżeli pozwalają na to zasoby organizacji - niezależności zespołu przeprowadzającego ocenę skutków w zakresie ochrony danych od zespołu pracującego nad samą aplikacją inteligentnej sieci. Przyczyni się do uczciwości i obiektywności tej oceny – dokument nie zawiera tego wymogu.

→ **Etap 3**

- W opisie systemu brakuje jasnego opisu aktywów, na których opiera się przetwarzanie danych osobowych (np. bazy danych pełniącej funkcję repozytorium danych zgromadzonych w danym obszarze). Byłoby to ważne, ponieważ niektóre z zagrożeń będą również dotyczyły tych aktywów. Wyczerpująco opisać trzeba także różne rodzaje przetwarzanych danych osobowych, jak również cele i sposoby przetwarzania tych danych. Proponowane okresy zatrzymywania tych danych także muszą być określone.

→ **Etap 4**

- Etap ten opiera się głównie na wykazie zagrożeń znajdującym się w kwestionariuszach zamieszczonych w szablonie oceny skutków w zakresie ochrony danych. Wydaje się, że pomylono zagrożenia z czynnikami ryzyka (zob. sekcja 2.2 niniejszej opinii). Ponadto niektóre wymienione elementy odnoszą się raczej do „braku środków" (np. niewystarczający mechanizm logowania, nieujednolicenie mechanizmu żądania dostępu przez osoby, których dane dotyczą) niż do zagrożeń.

→ **Etap 5**

- Skutki zagrożeń dla ochrony danych są ważone w kategoriach skutków dla celów w zakresie ochrony prywatności i danych, które określono w załączniku I, a nie pod względem skutków dla zainteresowanych osób (osób, których dane dotyczą). Ponadto sam szablon oceny skutków w zakresie ochrony danych nie zawiera wystarczających wytycznych odnośnie do rodzajów skutków i metodyki.
- Prawdopodobieństwo urzeczywistnienia się ryzyka jest opisane jako połączenie poziomu podatności z łatwością wykorzystania tej podatności. Ponieważ jednak na etapie 3 nie określono aktywów wspierających działania związane z danymi osobowymi, nic nie wskazuje na to, do czego odnosi się ta podatność.

→ **Etap 6**

- W szablonie oceny skutków w zakresie ochrony danych niezwykle istotne jest również wyraźne dopasowanie każdego ryzyka do co najmniej jednego odpowiedniego środka kontroli służącego ograniczeniu tego ryzyka (przy czym trzeba wyraźnie zaznaczyć, że w stosownych i odpowiednio uzasadnionych przypadkach niektóre rodzaje ryzyka mogą być również przeniesione lub akceptowane). Zależność ta powinna stać się głównym elementem dokumentu. Obecna struktura szablonu nie pozwala na zastosowanie takiego zintegrowanego podejścia, jak zauważyła Grupa Robocza Art. 29 już w swoim piśmie z października 2012 r.
- W odniesieniu do ryzyka szczątkowego (sekcja 6), jak Grupa Robocza Art. 29 wspomniała już w swoich uwagach z października 2012 r., prawo do ochrony danych osobowych jest prawem podstawowym, a przestrzeganie tego prawa jest jasnym i ważnym wymogiem prawnym. Powinno to być wyraźniej podkreślone w odniesieniu do możliwości akceptowania pewnego stopnia

ryzyka szczątkowego – można wyjaśnić, że bez względu na wynik każdej oceny ryzyka trzeba zrealizować cele w zakresie ochrony danych i prywatności, na przykład osoby, których dane dotyczą, muszą we wszystkich przypadkach otrzymywać stosowne powiadomienia oraz musi również istnieć zgodna z prawem podstawa przetwarzania (np. obowiązek prawny lub zgoda wyrażona przez osobę, której dane dotyczą). Ważne jest, żeby bardzo jasno dać do zrozumienia, że we wszystkich przypadkach trzeba przestrzegać przepisów o ochronie danych. Ocena ryzyka może pomóc w określeniu najlepszego sposobu zapewnienia zgodności z przepisami o ochronie danych, np. jaki rodzaj szyfrowania zastosować, aby zapewnić odpowiedni poziom bezpieczeństwa danych, jaki czas można uznać za proporcjonalny okres zatrzymywania danych lub jak najlepiej zminimalizować ilość gromadzonych i przetwarzanych danych. Ocena ryzyka nie powinna być jednak wykorzystywana jako pretekst do niespełnienia wymogów prawnych w przypadkach, w których ryzyko jest postrzegane jako stosunkowo niższe. W odniesieniu do tej kwestii Grupa Robocza Art. 29 ma uwagę o charakterze bardziej ogólnym - nie ma wskazówek dotyczących ustalania poziomu ryzyka szczątkowego, który można byłoby zaakceptować.

Załącznik II Wykaz możliwych środków kontroli

Środki kontroli wymienione w załączniku II nie są wystarczająco konkretne, aby stanowić przydatne wskazówki dla administratorów. W większości z nich nie uwzględnia się również specyfiki kontekstu inteligentnych sieci i nie odzwierciedlają one doświadczeń branży odnośnie do najważniejszych obaw i najlepszych praktyk.

W celu zilustrowania naszych oczekiwań związanych z poziomem szczegółowości i praktycznymi przykładami, jakich oczekujemy od szablonu, pragniemy podkreślić niektóre najważniejsze kwestie, które naszym zdaniem trzeba wyczerpująco uwzględnić w szablonie.

Podstawa prawna i wybór

Grupa Robocza Art. 29 chciałaby, aby szablon zawierał więcej wytycznych odnośnie do wyboru podstawy prawnej przetwarzania danych oraz wyboru, jaki należy zapewnić osobom, których dane dotyczą. Przede wszystkim powinny się w nim znajdować jasne wytyczne co do tego, co można zrobić bez zgody użytkownika, a co wymaga jego zgody. Szczególną uwagę należy zwrócić na wdrożenie systemu zdalnych wyłączników i odczytów granularnych[23].

W większości przypadków wymagana byłaby dobrowolna, konkretna, świadoma i wyraźna zgoda na każde przetwarzanie, które wykracza poza przetwarzanie potrzebne do (i) dostarczania energii, (ii) wystawiania faktur za energię, (iii) wykrywania oszustw polegających na nieodpłatnym korzystaniu z dostarczanej energii[24] oraz (iv) przygotowywania zagregowanych danych niezbędnych do energooszczędnej konserwacji sieci energetycznej (prognozowanie i rozliczanie)[25]. Do przykładów przypadków, w których zgoda byłaby wymagana, należy śledzenie i profilowanie na potrzeby ukierunkowanych reklam.

Aby zgoda była ważna, konsumenci muszą rozumieć, co dzieje się z ich danymi. Co ważne, w przypadku profilowania powinni mieć prawo znać swoje indywidualne profile oraz logikę i algorytmy wykorzystywane do eksploracji danych. Równie istotne są informacje na temat funkcji zdalnego włączania/wyłączania: klienci muszą wiedzieć, jakie zdarzenia mogą spowodować wyłączenie.

Ograniczanie ilości danych i technologie służące wzmocnieniu ochrony prywatności

Szablon oceny skutków w zakresie ochrony danych powinien zachęcać zainteresowane przedsiębiorstwa do zapewnienia gromadzenia i przetwarzania danych osobowych tylko w takiej ilości, jaka jest absolutnie niezbędna. W tym celu można rozważyć kilka metod. Zalecamy opisanie w szablonie oceny skutków w

[23] Zob. np. pkt 48 opinii EIOD z dnia 8 czerwca 2012 r., przywołanej w przypisie 3 powyżej.

[24] Oczywiście przetwarzanie danych w celu wykrywania oszustw nadal musi być zgodne z wszelkimi innymi stosownymi zabezpieczeniami ochrony danych, w tym z wymogiem proporcjonalności, oraz zasadą ograniczania ilości danych.

[25] W stosownych przypadkach te cele, dla których nie jest wymagana żadna zgoda, zazwyczaj są zbieżne z obowiązkami administratorów danych wynikającymi z przepisów.

zakresie ochrony danych – pokrótce i w sposób neutralny technologicznie - przynajmniej najbardziej rozpowszechnionych technologii służących wzmocnieniu ochrony prywatności i innych najlepszych dostępnych technik ograniczania ilości danych, a następnie opisanie ich bardziej szczegółowo w towarzyszącym dokumencie zawierającym BAT, który zostanie opracowany przez EG2, aby pomóc w promowaniu przyjaznego ochronie danych rozpowszechnianiu technologii inteligentnych pomiarów i inteligentnych sieci.

W szczególności istnieją innowacyjne technologie służące wzmocnieniu ochrony prywatności, obecnie znajdujące się na różnych etapach badania i rozwoju, które umożliwiają osiągnięcie podstawowych celów inteligentnego systemu pomiarowego (wystawianie faktur, energooszczędna konserwacja sieci (prognozowanie i rozliczanie) oraz zapewnienia bezpieczeństwa (w tym zapobieganie oszustwom) w sposób, który pozwoli w ogóle uniknąć - przynajmniej w odniesieniu do takich podstawowych celów – konieczności przekazywania szczegółowych odczytów z inteligentnych liczników w gospodarstwie domowym, w którym zainstalowano taki licznik. Poza tym można byłoby omówić następujące kwestie:

- Częstość odczytu liczników: naruszenie prywatności w dużym stopniu rośnie wraz ze wzrostem częstości odczytu liczników. Grupa Robocza Art. 29 chciałaby, żeby w szablonie oceny skutków w zakresie ochrony danych zostały uwzględnione dalsze wytyczne, w tym odniesienia[26] i przykłady związane z tym zagadnieniem.
- Dobór próby: stosowanie doboru próby (tj. gromadzenie danych tylko reprezentatywnego odsetka gospodarstw domowych) mogłoby pomóc w wyeliminowaniu gromadzenia i przetwarzania danych ze wszystkich gospodarstw w określonych celach (takich jak prognozowanie). Szablon oceny skutków w zakresie ochrony danych powinien zawierać również przykłady dotyczące doboru próby.
- Agregowanie połączone z usunięciem: w określonych celach, w tym na potrzeby prognozowania, powinno wystarczyć zatrzymywanie dokładnych odczytów z liczników wyłącznie do czasu obliczenia zagregowania. W takich przypadkach dane można trwale usuwać po zrealizowaniu tego celu. Ponownie należy przedstawić przykłady.
- Gromadzenie danych zagregowanych w pierwszej kolejności (zamiast gromadzenia poszczególnych danych i następnie agregowania tych danych): w przypadku niektórych celów (w tym pewnych celów związanych z prognozowaniem, konserwacją sieci i wykrywaniem oszustw) operatorowi sieci dystrybucji prądu elektrycznego lub gazu powinno wystarczyć gromadzenie danych z liczników, które nie mierzą zużycia w poszczególnych gospodarstwach domowych, a zamiast tego z liczników rozmieszczonych w takich lokalizacjach sieci dystrybucji, w których mogą mierzyć wyłącznie zagregowane zużycie w pewnej liczbie gospodarstw domowych (np. w bloku mieszkalnym, na ulicy lub w dzielnicy). W przypadku tych celów można całkowicie uniknąć gromadzenia szczegółowych danych dotyczących

[26] Zob. EG2.P.1 w „Essential Regulatory Requirements and Recommendations for Data Handling, Data Safety, and Consumer Protection" [Najważniejsze wymogi prawne i zalecenia dotyczące przetwarzania danych, bezpieczeństwa danych i ochrony konsumentów] (http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2_deliverable.pdf)

poszczególnych gospodarstw domowych. Ponownie pomocne będzie zamieszczenie w szablonie oceny skutków w zakresie ochrony danych ilustrujących przykładów z rzeczywistości, aby zachęcić do dążenia do zgodności z przepisami o ochronie danych i z dobrą praktyką.

- Aby pomóc zminimalizować nie tylko ilość gromadzonych danych, ale okres ich zatrzymywania, szablon oceny skutków w zakresie ochrony danych powinien zawierać również więcej wytycznych dotyczących okresów zatrzymywania. Naszym zdaniem, co do zasady, przechowywanie szczegółowych danych na temat konsumpcji indywidualnych gospodarstw domowych, zbieranych w celu wystawiania faktur, powinno być dopuszczalne jedynie do końca okresu, w którym istnieje możliwość zgodnego z prawem zakwestionowania faktury lub dochodzenia zapłaty (pozostaje to oczywiście bez uszczerbku dla prawa konsumenta do dłuższego okresu zatrzymywania w oparciu o zgodę, np. w celu uzyskania ukierunkowanego doradztwa energetycznego lub w innych możliwych celach zgodnych z prawem).

Glosariusz

Grupa Robocza Art. 29 zaleca poddanie glosariusza dokładnemu przeglądowi w celu zapewnienia zgodności terminologii z aktualnym brzmieniem dyrektywy 95/46/WE, a także z proponowanymi nowymi ramami ochrony danych,