GRUPA ROBOCZA ART. 29

2064/13/PL
WP209

Opinia 07/2013 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

Grupa robocza została powołana 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 Komisji Europejskiej, B-1049 Bruksela, Belgia, biuro nr MO-59 02/013.

Strona internetowa: http://ec.europa.eu/justice/data-protection/index_en.htm

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 2012/148/UE 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 członkowskie powinny dopilnować, aby operatorzy sieci i operatorzy inteligentnych systemów pomiarowych przedsięwzięli odpowiednie środki techniczne i

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.

organizacyjne w celu zapewnienia ochrony danych osobowych zgodnie ze sprawozdaniem dotyczącym oceny skutków w zakresie ochrony danych opracowanym w oparciu o stosowanie szablonu, uwzględniając opinię Grupy Roboczej Art. 29 na temat tego szablonu[3].

Komisja ponadto przewiduje w zaleceniu, że w ocenie skutków w zakresie ochrony danych należy ująć „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. EG2, która składa się głównie z przedstawicieli branży, zorganizowała od tamtej pory kilka warsztatów, w których przedstawiciele Grupy Roboczej Art. 29 brali udział w charakterze obserwatorów.

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.

Pierwsza wersja szablonu oceny skutków w zakresie ochrony danych

W dniu 8 stycznia 2013 r. Komisja przedłożyła Grupie Roboczej Art. 29 pierwszą 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[4].

Grupa Robocza Art. 29 wydała opinię nr 04/2013 w dniu 22 kwietnia 2013 r. Z jednej strony w opinii tej podziękowano zainteresowanym stronom z EG2 za przeprowadzenie szeroko zakrojonych prac i z zadowoleniem przyjęto ustalone cele.

---

[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] 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.

Z drugiej strony określono kilka krytycznych problemów, które można podsumować w następujący sposób:

(i) brak przejrzystości co do charakteru i celów oceny skutków w zakresie ochrony danych;

(ii) błędy metodologiczne w szablonie oceny skutków w zakresie ochrony danych;

(iii) brak 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.

Grupa Robocza Art. 29 stwierdziła, że szablon oceny skutków w zakresie ochrony danych nie jest wystarczająco dojrzały i dopracowany, i poprosiła Komisję o zapewnienie kontynuacji prac nad szablonem oceny skutków w zakresie ochrony danych w celu zagwarantowania, że administratorzy danych ostatecznie otrzymają wystarczająco szczegółowe, użyteczne i jasne praktyczne wytyczne.

Grupa Robocza Art. 29 poprosiła również Komisję, żeby rozważyła włączenie do szablonu oceny skutków w zakresie ochrony danych najlepszych dostępnych technik (BAT, które zdefiniowano w pkt 3 lit. f) zalecenia) i przedłożenie połączonego dokumentu Grupie Roboczej Art. 29 do zaopiniowania. Zaleciła ponadto, aby Komisja rozważyła sporządzenie bilansu wcześniejszych i obecnych prac w dziedzinie oceny skutków w zakresie ochrony danych i rozważyła możliwość określenia ogólnej metodyki dokonywania takiej oceny, która mogłaby być przydatna w pracach związanych z określonym obszarem.

Druga wersja szablonu oceny skutków w zakresie ochrony danych

Komisja odpowiedziała na opinię Grupy Roboczej Art. 29 w dniu 27 maja 2013 r. W swoim piśmie Komisja zwróciła się do EG2 o zmieniony szablon i przyznała, że pewnego wsparcia EG2 w jej pracy może udzielić Grupa Robocza Art. 29, zachowując jednocześnie swoją szczególną rolę. Ponadto Komisja wolała nie włączać najlepszych dostępnych technik do szablonu – jak twierdzi – ze względu na to, że ich zakres ogranicza się do wspólnych minimalnych wymogów funkcjonalnych dotyczących inteligentnych systemów pomiarowych i ich rozwojowego charakteru[5]. W sprawie wniosku dotyczącego określenia ogólnej metodyki oceny skutków w zakresie ochrony danych, która to metodyka byłaby przydatna w inicjatywach związanych z konkretnymi dziedzinami, w piśmie zwrócono się do innego właściwego departamentu Komisji, od którego dotychczas nie otrzymano odpowiedzi.

[5] „Uważam, że nie byłoby tak korzystne, jak Pan zakłada, z następujących powodów: (i) zgodnie z zaleceniem Komisji 2012/148/EU najlepsze dostępne techniki dotyczą tylko wspólnych minimalnych wymogów funkcjonalnych dotyczących inteligentnych systemów pomiarowych, podczas gdy zakres stosowania szablonu oceny skutków w zakresie ochrony danych ma wykraczać poza „ostatnią milę" i obejmować całe spektrum inteligentnych sieci; oraz (ii) w przypadku włączenia najlepszych dostępnych technik do szablonu oceny skutków w zakresie ochrony danych ich rozwojowy i ilustracyjny charakter tym samym sprawi, że szablon będzie miał charakter efemeryczny i że konieczne mogą być niepraktycznie częste jego zmiany".
(pismo ener.b.3 VL/cv(2013)1506536 do pana Kohnstamma, z dnia 27 maja 2013 r.).

Na potrzeby drugiego projektu szablonu EG2 utworzyła zespół redakcyjny, który spotkał się w dniach 4 czerwca i 3 lipca 2013 r. Niektórzy przedstawiciele Grupy Roboczej Art. 29 uczestniczyli w pierwszym spotkaniu w charakterze obserwatorów i odpowiedzieli na pytania przedstawicieli EG2 na temat różnych kwestii poruszonych w szablonie.

W dniu 20 sierpnia 2013 r. Komisja przedłożyła Grupie Roboczej Art. 29 ostateczną wersję szablonu oceny skutków w zakresie ochrony danych przygotowanego przez członków EG2.

Struktura niniejszej opinii

W sekcji 1 zawarto opis zdarzeń prowadzących do powstania zmienionego szablonu oceny skutków w zakresie ochrony danych; przywołano w niej też sekcje opinii 04/2013 w odniesieniu do kwestii ochrony danych w inteligentnych sieciach i celów oceny skutków w zakresie ochrony danych w tym kontekście.

Sekcja 2 zawiera ocenę zmienionego szablonu oceny skutków w zakresie ochrony danych dokonaną przez Grupę Roboczą Art. 29.

W sekcji 3 wyciągnięto ostateczne wnioski.

1.2 Ochrona danych w inteligentnych sieciach i cele oceny skutków w zakresie ochrony danych w tym kontekście

Kwestie ochrony danych w inteligentnych sieciach i celów oceny skutków w zakresie ochrony danych w tym kontekście zostały już uwzględnione w sekcjach 1.2 i 1.3 opinii nr 04/2013. Grupa Robocza Art. 29 nie ma żadnych nowych elementów do dodania w odniesieniu do tych kwestii.

2 Analiza szablonu oceny skutków w zakresie ochrony danych

Grupa Robocza Art. 29 z zadowoleniem przyjmuje prace przeprowadzone przez członków EG2 w celu odniesienia się do uwag Grupy Roboczej Art. 29 i ich chęć uwzględnienia porad Grupy Roboczej Art. 29 jako cennego wsparcia.

Niniejsza analiza stanowi głównie uzupełnienie uwag zawartych w opinii 04/2013. Obejmuje również rozwiązania w zakresie ulepszeń i optymalizacji, które należy rozważyć w celu ukończenia prac nad szablonem. W poniższych sekcjach uwzględniono oba aspekty.

Aby uzyskać dogłębne i jasne zrozumienie, niniejszą analizę należy interpretować w świetle treści i terminologii opinii 04/2013.

2.1 Szablon oceny skutków w zakresie ochrony danych i zalecenie KE 2012/148/UE

Grupa Robocza Art. 29 skorzystała z okazji, by uważnie przeanalizować tę drugą wersję szablonu oceny skutków w zakresie ochrony danych na potrzeby inteligentnych sieci w świetle zalecenia Komisji, w którym określono cel, zakres i zastosowanie tego szablonu.

2.1.1 Uznaniowy charakter przeprowadzania oceny skutków w zakresie ochrony danych na potrzeby inteligentnych sieci

Podczas gdy z jednej strony istnienie zalecenia Komisji nie nakłada prawnie wiążącego obowiązku, to z drugiej strony w zaleceniu tym stwierdzono, że pewne środki są zdecydowanie zalecane. Zalecenie 2012/148/UE stanowi, że w operacjach przetwarzania danych osobowych w inteligentnych licznikach/inteligentnych sieciach potrzebny jest „uporządkowany proces oceny ewentualnych skutków zagrożeń [...] dla praw i wolności osób, których dotyczą dane, ze względu na ich charakter, zakres lub cel". Grupa Robocza Art. 29 chce potwierdzić, że potrzeba takiego procesu, wskazana już w opinii 12/2011 Grupy Roboczej Art. 29 na temat inteligentnego pomiaru zużycia (*smart metering*) w kontekście podejścia polegającego na uwzględnieniu ochrony prywatności już w fazie projektowania, jest w dużej mierze uzasadniona złożonością infrastruktury technicznej i zarządczej inteligentnych sieci, jej potencjalną skalą zastosowania i rozwoju, jak również konkretnymi zagrożeniami dla podstawowych praw i wolności jednostki, w tym między innymi dla życia (np. wyłączenie dostaw energii elektrycznej w sytuacji, w której pewne maszyny zasilane energią elektryczną podtrzymują funkcje życiowe).

Ponadto Grupa Robocza Art. 29 z zadowoleniem przyjęła fakt, że Komisja przedstawiła wniosek dotyczący ogólnego rozporządzenia o ochronie danych, zgodnie z którym w określonych warunkach ocena skutków w zakresie ochrony danych byłaby obowiązkowa. Dla zainteresowanych stron w odniesieniu do szablonu oceny skutków w zakresie ochrony danych na potrzeby inteligentnych sieci, czyli administratorów danych i podmiotów przetwarzających, powinno być jasne, że stosowanie szablonu należy postrzegać jako sposób wywiązywania się z obowiązku prawnego w przyszłości. Biorąc pod uwagę ogromne inwestycje i długi horyzont planowania sieci mediów, należy zrozumieć, że gromadzenie doświadczenia związanego z podejściem opartym na ocenie skutków w zakresie ochrony danych i stosowanie go już od początku w projektowaniu systemów leży w prawdziwym interesie zainteresowanych stron, tak by nie napotkały one problemów ze zgodnością, gdy opracowywane obecnie prawodawstwo wejdzie w życie. W przypadku gdy sformułowania zastosowane w obecnym szablonie, zwłaszcza w sekcji 2.1, można byłoby interpretować jako pozostawiające przedsiębiorstwom znaczny margines swobody, Komisja powinna dopilnować, aby podano wyjaśnienie, że margines ten należy interpretować w sposób ścisły, np. wyjaśniając to podejście w zaleceniu Komisji, które może towarzyszyć szablonowi i pomagać w jego stosowaniu; ma to służyć zagwarantowaniu, że faktyczna ocena skutków w zakresie ochrony danych przeprowadzana jest w możliwie najbardziej wyczerpujący sposób. Grupa Robocza Art. 29 interpretuje rolę oceny wstępnej jako funkcjonalną, aby uwzględnić wszystkie możliwe sytuacje, w których mogą znaleźć się potencjalni administratorzy danych i podmioty przetwarzające, w oparciu o przetworzone informacje, zakres analizowanego (pod)systemu, status projektu itp., a nie jako etap metodyki osłabiający cele zalecenia Komisji.

2.1.2 Ocena skutków w zakresie ochrony danych i organy ochrony danych

Punkt 8 zalecenia Komisji stanowi, że państwa członkowskie powinny dopilnować, aby przed przetwarzaniem podmiot przetwarzający dane osobowe konsultował się z organem ochrony danych w sprawie oceny skutków w zakresie ochrony danych. Grupa Robocza Art. 29 zwraca uwagę, że w wielu częściach szablonu podejście to nie

jest w pełni odzwierciedlone. Niektóre z cytatów: „w razie wątpliwości" (sekcja 2.1.4), lub – należy po prostu skonsultować się z inspektorem ochrony danych (a nie z organem ochrony danych), „jeśli jest dostępny" (sekcja 2.6.2), lub – przedłożyć organowi ochrony danych „na żądanie", gdy sprawozdanie końcowe zostanie przyjęte (sekcja 2.7). Chociaż lepiej byłoby konsekwentnie wyjaśnić w szablonie, że przed przetwarzaniem należy zasięgnąć opinii krajowych organów ochrony danych zgodnie z zaleceniem Komisji, chyba że krajowe przepisy o ochronie danych lub krajowa polityka organu ochrony danych przewidują jasno wyjątek, to Komisja powinna zagwarantować w odpowiedni sposób, by zainteresowane strony miały jasność co do tego, że szablon oceny skutków w zakresie ochrony danych przyjęty zgodnie z zaleceniem Komisji nie może sam w sobie zmieniać zasad przyjętych w zaleceniu. Przywołane fragmenty można rozumieć tylko jako informujące o dodatkowych możliwościach uzyskania porad, które to możliwości stanowią uzupełnienie konsultacji z organami ochrony danych zgodnie z zaleceniami Komisji.

2.2 Przejrzystość co do charakteru i celów oceny skutków w zakresie ochrony danych

2.2.1 Uwzględnienie ostatecznych skutków dla praw i wolności jednostki

Grupa Robocza Art. 29 z zadowoleniem przyjmuje fakt, że etap oceny ryzyka w ramach metodyki przedstawionej w szablonie (sekcja 2.5) ma na celu uwzględnienie faktycznych skutków dla podstawowych praw, wolności i swobód obywatelskich osób, których dane dotyczą (takich jak na przykład straty finansowe lub dyskryminacja cenowa, lub przestępstwa ułatwione przez nieupoważnione profilowanie), jako efektów „zdarzeń, co do których istnieją obawy", wynikających z nieuczciwego i niezgodnego z prawem przetwarzania danych osobowych, a nie skutków dla celów w zakresie ochrony prywatności jako takich.

Niemniej jednak wydaje się, że w tekście wyjaśniającym metodykę oceny ryzyka wciąż panuje pewien zamęt (zob. odpowiednia sekcja niniejszej opinii), a szczególnie w sekcji 2.5.1.1 szablonu, gdzie opisano, jak ocenić skutki zdarzeń, co do których istnieją obawy. W szczególności żadnej jasności nie zapewnia zdanie, w którym próbuje się określić elementy na potrzeby oceny „skutków i powagi pewnych zidentyfikowanych zagrożeń". Cele w zakresie ochrony prywatności wspomniane są w tym tekście jako elementy tej oceny (zob. sekcja **Error! Reference source not found.** niniejszej opinii), lecz nie omówiono ich szczegółowo i nie wyjaśniono, jaka jest ich funkcja, „ryzyko związane z przestępczością" wyróżniono bez wyraźnego powodu i wymieniono odrębnie takie elementy, jak „swoboda przemieszczenia się, utrata niezależności, utrata równości", nazywając je „innymi zasadami ochrony prywatności"[6].

[6] Można zaproponować uzupełnienie akapitu pierwszego ostatnie zdanie sekcji „2.5.1.1. Skutki zdarzeń, co do których istnieją obawy" o inne elementy i sformułowanie go następująco: „Ten potencjalny skutek jest definiowany przez konsekwencje, jakie każde zdarzenie, co do którego istnieją obawy, może mieć dla prywatności i innych podstawowych praw i wolności osób, których dane dotyczą, w tym np. ryzyko związane z przestępczością, takie jak kradzież tożsamości i nadużycia finansowe, lub dla swobody przemieszczania się, niezależności, równego traktowania, relacji społecznych, interesów finansowych itp. ze względu na np. profilowanie, niezamówiony marketing, dyskryminację lub indywidualne decyzje w oparciu o błędne informacje...".

Grupa Robocza Art. 29 pragnie podkreślić, że w ocenie skutków w zakresie ochrony danych zawsze i konsekwentnie ocenia się skutki dla „praw i wolności osoby, której dane dotyczą", jak przypomniano w sekcji 2.1 opinii 04/2013, i prawidłowo stwierdzono w kilku częściach szablonu. W przypadku gdy w szablonie stosowana jest odmienna terminologia, np. odnosząca się jedynie do prawa do prywatności, trzeba ją interpretować jako odniesienie do bardziej kompleksowego pojęcia. Powinno to zostać uwzględnione w przyszłych zmianach szablonu.

Ponadto, jeśli prawdą jest, że to samo zdarzenie, co do którego istnieją obawy, może prowadzić do wielu skutków dla osób, których dane dotyczą, przydatne może być – dla celów poszerzenia wiedzy i określenia rozmiarów skutków - wymienienie w przykładach podanych w sekcji 3.4.1 najistotniejszych skutków dla osób, których dane dotyczą, w związku ze zdarzeniami, co do których istnieją obawy. Ten związek między zdarzeniem, co do którego istnieją obawy, a skutkami dla podstawowych praw i wolności jednostki jest charakterystyczny dla przedmiotowych działań w kontekście ochrony osób fizycznych pod względem przetwarzania danych osobowych w przeciwieństwie na przykład do zwykłej oceny zagrożeń dla bezpieczeństwa informacji.

2.2.2 Uwzględnianie celów w zakresie ochrony prywatności

Sposób uwzględniania celów w zakresie ochrony prywatność jest jedną z najważniejszych kwestii w ocenie skutków w zakresie ochrony danych. Jej celem jest zagwarantowanie, że cele w zakresie ochrony prywatności zostały prawidłowo wzięte pod uwagę.

Obecnie cele w zakresie ochrony prywatności są następujące:

- wspomniane w sekcji „2.5.1.1 Skutki zdarzeń, co do których istnieją obawy" jako elementy, które należy uwzględnić przy ocenie skutków i powagi określonych zidentyfikowanych zagrożeń;
- wspomniane w sekcji „2.6.3. Ryzyko szczątkowe i akceptacja ryzyka" jako cele, które należy osiągnąć;
- wymienione i opisane w „Załączniku 1. Cele w zakresie ochrony prywatności i danych".

W większości przepisów dyrektywy 95/46/WE[7] określono szczególne warunki dotyczące przetwarzania danych osobowych oraz zbiór obowiązków, do których administratorzy danych i podmioty przetwarzające muszą się stosować. W dyrektywie tej nie przewidziano marginesu swobody ani dopuszczalnego poziomu niezgodności z tymi przepisami. W dyrektywie zapewniono bezpieczeństwo przetwarzania danych jako jeden z tych obowiązków, a w celu jego wykonania w art. 17 dyrektywy przewidziano podejście do zarządzania ryzykiem; artykuł ten stanowi, że „[u]względniając stan wiedzy w tej dziedzinie oraz koszt realizacji, przyjęte zostaną takie środki, które zapewnią poziom bezpieczeństwa odpowiedni do zagrożeń wynikających z przetwarzania danych oraz charakteru danych objętych ochroną". W

[7] 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.

kontekście szablonu oceny skutków ważne jest, aby mieć świadomość, że strategie zarządzania ryzykiem, np. opracowane w dziedzinie bezpieczeństwa, mogą być stosowane do ochrony danych, ale jedynie w odniesieniu do kwestii bezpieczeństwa, oraz że w przypadku większości obowiązków wymagana jest pełna zgodność. W szablonie na potrzeby wyznaczenia obowiązków dotyczących zgodności użyto terminu „cele w zakresie ochrony prywatności" oraz wyjaśniono w sekcji 2.6.3, że pojęcia ryzyka szczątkowego i akceptacji ryzyka nie mają zastosowania do tych celów w zakresie ochrony prywatności, które „muszą zostać osiągnięte" (str. 33).

Grupa Robocza Art. 29 z zadowoleniem przyjmuje fakt, że w szablonie odróżniono zarządzanie ryzykiem od zgodności, lecz wolałaby, aby było to przedstawione w sposób jaśniejszy i bardziej widoczny.

Zawsze powinny zatem istnieć dwa różne i uzupełniające się działania w celu odniesienia się do ustaleń poczynionych w ramach oceny skutków w zakresie ochrony danych. Pierwsze działanie jest związane z ryzykiem dla danych osobowych. Ryzyko to powinno być objęte zarządzaniem ryzykiem (ocenione, odpowiednio potraktowane itp.). Drugie działanie dotyczy zgodności z celami w zakresie ochrony prywatności jako obowiązkami prawnymi. Należy to uznać za kwestie zgodności (środki wdrożone lub planowane, aby osiągnąć cele w zakresie ochrony prywatności, uzasadnienie, jeżeli nie osiągnięto tych celów, zagrożenia prawne związane z nieosiągnięciem tych celów, planowane kontrole, aby sprawdzić, czy i jak cele te są osiągane lub nie...).

Jeśli chodzi o analizę ryzyka, należy podkreślić, że opisane w sekcji „2.4.1. Wprowadzenie" zdarzenia, co do których istnieją obawy, powinny być systematycznie oceniane. Należy określić ich potencjalne skutki dla osób, których dane dotyczą, a oszacowanie negatywnych skutków powinno być oparte na tych potencjalnych skutkach. Niemniej jednak Komisja może chcieć sprawdzić, co odróżnia ostatnie zdarzenie, co do którego istnieją obawy (przekazanie danych osobowych [...] osobom, którym nie są one potrzebne), od trzeciego (nieuprawniony dostęp do danych osobowych [...] przez osoby nieupoważnione).

W celu ułatwienia stosowania metodyki zaproponowanej w szablonie Grupa Robocza Art. 29 chce zaproponować kilka narzędzi uzupełniających. Zwraca się do Komisji, aby poinformowała o tych propozycjach potencjalnych użytkowników szablonu, np. poprzez udostępnienie niniejszej opinii z szablonem lub umieszczenie odesłania do niej w jakimkolwiek dokumencie towarzyszącym. Narzędzia uzupełniające opisano w załączniku do niniejszej opinii.

2.3 Metodyka zastosowana w szablonie oceny skutków w zakresie ochrony danych

Ogólnie metodyka przedstawiona w szablonie została wyjaśniona i jest łatwiejsza do wykonania. Nadal jednak pozostaje wiele niejasnych i mylących elementów, w tym w wykazie ogólnych zagrożeń przedstawionych w sekcji 3.4.1, w formularzach szablonu oraz w kwestionariuszu.

Niektóre z tych elementów omówiono w sekcji 2.1 w kontekście przejrzystości charakteru i celów oceny skutków w zakresie ochrony danych. Inne zostaną uwzględnione w niniejszej sekcji.

2.3.1 Metodyka oceny ryzyka (zarządzania oceną ryzyka)

Większość elementów metodyki zarządzania ryzykiem opiera się głównie na normie ISO 31 000, metodyce EBIOS oraz syntezie opracowanej przez CNIL[8].

Identyfikacja aktywów

Określenie aktywów podstawowych i wspierających stanowi cel ogólnej oceny ryzyka.

Określenie i ocena zagrożeń i słabych stron

Obecnie określono różnicę między zagrożeniami a ryzykiem. Zwiększono ilość wytycznych dotyczących pojęcia słabych stron.

Grupa Robocza Art. 29 jest jednak zaniepokojona faktem, że przedstawienie pominiętych celów w zakresie ochrony prywatności jako zagrożeń ogólnych wymienionych w sekcji 3.4.1, a w szczególności w sekcji 3.4.1.4, może prowadzić do nieporozumienia, iż w szablonie „pominięty cel w zakresie ochrony prywatności zdefiniowany jest jako zagrożenie", aby odpowiadał ocenie celów w zakresie ochrony prywatności w kontekście metodyki oceny ryzyka. Problem ten został już omówiony w sekcji **Error! Reference source not found.** niniejszej opinii.

Grupa Robocza Art. 29 przyznaje jednak, że zapewnione odpowiednie przykłady i wytyczne (na potrzeby zapisów tabel w sekcji 3.4.1, w których opisuje się pominięte cele w zakresie ochrony prywatności) są nadal przydatne w pozostałych kolumnach - po poprawieniu - dla zrealizowania właśnie tych celów w zakresie ochrony prywatności. Grupa Robocza Art. 29 proponuje, by wykorzystać te informacje w kontekście szerszego i bardziej szczegółowego podejścia do celów w zakresie ochrony prywatności (zob. także uwagi na końcu sekcji **Error! Reference source not found.** niniejszej opinii), aby zapewnić wytyczne dotyczące sposobu realizacji tych celów. Mogą one zostać przedstawione albo w postaci tabelarycznej lub – co być może jest lepszym rozwiązaniem - w specjalnej sekcji, w której wytyczne można by podać również w kontekście ryzykownych operacji przetwarzania danych (np. profilowania lub decyzji podejmowanych w odniesieniu do osób fizycznych w oparciu o zautomatyzowane operacje przetwarzania danych).

Obliczanie ryzyka/szeregowanie ryzyka pod względem ważności

Istnieją jaśniejsze wytyczne dotyczące sposobu obliczania ryzyka i szeregowania go pod względem ważności. Sekcja dotycząca obliczania ryzyka (2.5.1.3) wymaga lepszego sformułowania i większej jasności.

Traktowanie ryzyka

[8] http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf

Sekcję „2.6.1. Zmiana ryzyka: wdrożone i zaplanowane środki kontroli" należy włączyć do sekcji „2.5. Etap 5 – Ocena ryzyka dla ochrony danych" i uwzględnić w pierwszym oszacowaniu ryzyka. W tytule nie należy jednak wymieniać „zmiany ryzyka", która jest jedną z możliwości traktowania ryzyka. Tytuł mógłby po prostu brzmieć „Wdrożone i zaplanowane środki kontroli". Następnie w sekcji „2.6. Etap 6 – Określenie środków kontroli i ryzyka szczątkowego oraz zalecenia w tym zakresie", a zwłaszcza w sekcji „2.6.2. Traktowanie ryzyka", określane są dodatkowe środki kontroli, a ryzyko szacowane jest ponownie jako ryzyko szczątkowe.

W opinii 04/2013 Grupa Robocza Art. 29 zauważyła, że w pierwszej wersji szablonu czynniki ryzyka, które należy ograniczyć, nie są dopasowane do wykazu możliwych środków kontroli zawartego w załączniku II. Grupa Robocza Art. 29 z zadowoleniem przyjmuje fakt, że w nowej wersji szablonu opis celu możliwych środków kontroli często obejmuje rodzaj ryzyka, które zasadniczo ma ograniczać. Ponadto w niewyczerpującym wykazie ogólnych zagrożeń zawartym w sekcji 3.4.1 zagrożenia te powiązano z możliwymi środkami kontroli wymienionymi w załączniku II.

Ryzyko szczątkowe

Dla zrównoważenia wagi ryzyka szczątkowego na koniec procesu zarządzania ryzykiem równie ważne jest określenie na wczesnym etapie wszystkich zaangażowanych interesów. Można je określić w oparciu o ogólny proces zarządzania ryzykiem w przedsiębiorstwie, jeżeli taki istnieje. Reprezentowane mogą być nie tylko interesy gospodarcze czy inne uzasadnione interesy, lecz także inne kwestie, np. odpowiedzialność społeczna lub zgodność z innymi wymogami prawnymi.

Grupa Robocza Art. 29 proponuje dodanie nowej sekcji na potrzeby określania interesów istniejących w ramach przetwarzania danych. Sekcja ta mogłaby znajdować się pomiędzy sekcjami 2.3.1 i 2.3.2 i być zatytułowana „2.3.2. Interesy w ramach przetwarzania danych". Powinien być w niej wymagany opis możliwości utworzenia przetwarzania w inteligentnych sieciach (dla celów marketingowych/gospodarczych, społecznych, zgodności z prawem itd.).

Po akapicie pierwszym sekcji „2.6.4. Rozwiązanie" można by dodać ocenę ryzyka szczątkowego w odniesieniu do interesów. W akapicie tym można by wyjaśnić, że rozwiązanie polega na podjęciu decyzji o zaakceptowaniu lub niezaakceptowaniu ryzyka szczątkowego z uwzględnieniem interesów określonych w sekcji 2.3.

2.3.2 Role i obowiązki

Grupa Robocza Art. 29 z zadowoleniem przyjmuje włączenie do szablonu (sekcja 1.4.2) wykazu różnych typów operatorów inteligentnych sieci, w tym ogólnego opisu celów, w których mogą oni przetwarzać dane osobowe.

Obecność konkretnej podsekcji 2.1.2 lepiej uwydatnia obecnie potrzebę wyraźnego podziału obowiązków administratora danych i podmiotu przetwarzającego. Przykład zawarty w tekście obowiązków administratora danych i ewentualnego podmiotu przetwarzającego w inteligentnym systemie pomiarowym należy zintegrować poprzez inne przykłady dotyczące bardziej złożonych sytuacji. W tekście szablonu podany jest kolejny przykład (operator mikrosieci i zaangażowany zakład ubezpieczeń), w którym przedstawiony został problem, ale nie podano wytycznych.

Ponadto, jak już zaproponowano w opinii 04/2013, szablon oceny skutków w zakresie ochrony danych mógłby zawierać w ramach trzeciego etapu czwartą sekcję, która dotyczyłaby określania różnych obowiązków poszczególnych podmiotów zaangażowanych w przetwarzanie danych (do czego istnieje już odpowiedni formularz w sekcji 3).

2.3.3 Formularze szablonu

Poza innymi uwagami przedstawionymi w innych sekcjach niniejszej opinii Grupa Robocza Art. 29 pragnie uwydatnić niektóre kolejne niedociągnięcia w sekcjach zawierających opis niektórych formularzy stosowanych do przeprowadzenia oceny skutków w zakresie ochrony danych.

Na przykład w sekcji 3.3, która dotyczy związku pomiędzy różnymi szablonami stosowanymi do określenia, scharakteryzowania i opisania systemów inteligentnych sieci, kolejność i dokładny sposób stosowania tych szablonów są niejasne. Podane jest odesłanie do zewnętrznego dokumentu, lecz nie ma żadnego komentarza na temat celu tego odniesienia. Bądź też nie ma w metodyce odniesienia do sytuacji, w której należy wykorzystać formularz zawarty w sekcji 3.3.5.

Z drugiej strony tabela z aktywami pierwotnymi i odpowiednimi aktywami wspierającymi jest ważna dla pokierowania oceną ryzyka.

Zasadniczo należy zamieścić więcej wytycznych dotyczących stosowania formularzy. Bardzo przydatne byłoby podanie co najmniej jednego przykładu w załączniku.

2.4 Treści odnoszące się do danego sektora w szablonie oceny skutków w zakresie ochrony danych

Jedną z głównych kwestii wspomnianych w opinii 04/2013 był fakt, że czynniki ryzyka i środki kontroli przedstawione w pierwszej wersji szablonu nie odzwierciedlały doświadczeń branży odnośnie do najważniejszych obaw i najlepszych praktyk.

Grupa Robocza Art. 29 stwierdza i z zadowoleniem przyjmuje fakt, że niektóre określone treści zostały dodane do niewyczerpującego wykazu ogólnych zagrożeń w sekcji 3.4.1.1, zwłaszcza w kolumnie opatrzonej nagłówkiem „Przykłady konkretnych słabych stron w aktywach wspierających dotyczące sektora energetycznego”. Grupa Robocza Art. 29 uważa jednak, że potrzebne są pewne poprawki i dalsze wytyczne zarówno w tekście, jak i w szablonie, zwłaszcza na potrzeby zrealizowania celów w zakresie ochrony prywatności (zob. także sekcja **Error! Reference source not found.**).

Jak przypomniano w sekcji 1.1, Komisja odrzuciła wniosek Grupy Roboczej Art. 29 dotyczący włączenia do szablonu produktu w postaci najlepszych dostępnych technik (BAT), nad którymi pracuje EG2, ze względu na to, że ich zakres – jak twierdzi Komisja – ogranicza się do inteligentnych liczników, oraz z uwagi na ich rozwojowy charakter.

Grupa Robocza Art. 29 potwierdza swój pogląd, że uznanie najlepszych dostępnych technik za produkt nieodłącznie związany z szablonem umożliwiłoby organizacji

przeprowadzającej ocenę skutków w zakresie ochrony danych wybranie w razie konieczności odpowiednich środków. Rozwojowy charakter najlepszych dostępnych technik nie jest sprzeczny z ich uzupełniającą rolą w stosunku do szablonu oceny skutków w zakresie ochrony danych. Ponadto sam szablon będzie wymagał cyklu przeglądów w celu zachowania i udoskonalenia metodyki po pierwszym etapie stosowania, a w każdym razie okresowo. Fakt, że zakres najlepszych dostępnych technik jest ograniczony do inteligentnych liczników, a tym samym nie jest wyczerpujący, również nie jest powodem do wykluczenia ich stosowania z oceny skutków w zakresie ochrony danych. Inteligentne liczniki stanowią podsystemy, w których dane osobowe są przede wszystkim gromadzone i przetwarzane; a w każdym razie lepiej dysponować pewnymi wytycznymi, niż nie mieć ich w ogóle. Korzystając z okazji, Grupa Robocza Art. 29 proponuje ponadto, by Komisja i sektor przemysłu zbadały możliwość rozszerzenia cennych prac nad najlepszymi dostępnymi technikami również o szerszy zakres inteligentnych sieci.

W opinii 04/2013, a w szczególności w załączniku II, Grupa Robocza Art. 29 zaleciła opisanie w szablonie oceny skutków w 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. Nie zostało to zrealizowane. Grupa Robocza Art. 29 w dalszym ciągu uważa, że dla sektora przemysłu bardzo przydatne byłoby zarówno dysponowanie wachlarzem środków gotowych do wdrożenia, jak również posiadanie większej wiedzy o technologiach służących wzmocnieniu ochrony prywatności, aby tworzyć dalsze odpowiednie środki kontroli.

2.5 Potrzeba testowania/walidacji szablonu oceny skutków w zakresie ochrony danych

Grupa Robocza Art. 29 proponuje przeprowadzenie odpowiednich testów/walidacji szablonu oceny skutków w zakresie ochrony danych w terenie w oparciu o istniejącą wersję i w miarę możliwości z uwzględnieniem powyższych uwag. Grupa Robocza Art. 29 sugeruje, aby po przeprowadzeniu tych testów dokonano przeglądu szablonu i jego metodyki oraz poprawiono je w świetle tych doświadczeń i z uwzględnieniem wyżej wspomnianych uwag. Te przypadki testów, o których Grupa Robocza Art. 29 powinna zostać poinformowana i w których poszczególne organy ochrony danych mogą rozważyć zaoferowanie wsparcia, mogą również być pomocne pod względem dostarczenia cennych przykładów, które można byłoby włączyć do załączników do szablonu, aby zapewnić lepsze zrozumienie proponowanej metodyki.

2.6 Inne uwagi

2.6.1 Pojęcie danych osobowych

W sekcji 2.1 opisano, w jaki sposób ustalić, czy w analizowanym podsystemie inteligentnej sieci przetwarzane są dane osobowe. Grupa Robocza Art. 29 zwraca uwagę, że zaklasyfikowanie danych w wymienionych przykładach jako danych osobowych wydaje się poprawne, chociaż w uzasadnieniu podanym na potrzeby określenia informacji jako danych osobowych terminologia prawna nie zawsze jest ściśle stosowana.

Na przykład tak zwane „dane na temat zużycia” są uważane za dane osobowe, ponieważ „zapewniają wgląd w codzienne życie danej osoby fizycznej”, podczas gdy są one danymi osobowymi tylko dlatego, że odnoszą się do osoby, która zawarła umowę, oraz do jej ewentualnej rodziny. Fakt, że dane te zapewniają wgląd w codzienne życie, stanowi skutek dla prywatności. Uwaga ta dotyczy także innych pozycji wymienionych w szablonie. Chociaż wykaz przykładów jest z pewnością pomocny dla potencjalnych użytkowników szablonu, sprawia wrażenie, że aby uznać dane za dane osobowe, potrzebne są znaczne skutki dla prywatności. Ponadto powinno być jasne, że wykaz przykładów nie jest wyczerpujący.

2.6.2 Inne uwagi na temat terminologii dotyczącej ochrony danych

W niektórych sekcjach szablonu używane są takie terminy, jak „właściciel systemu”, który to termin jest znaczący pod względem stosowania, ale nie zawsze wyjaśnia związek z terminologią dotyczącą ochrony danych, która może mieć zastosowanie (na przykład „administrator danych”) (s. 14, 18, 32, [...]), czy też terminy „osoba fizyczna”, „konsument”, „klient”, które stosuje się bez wyraźnego odniesienia do osoby, której dane dotyczą (s. 10, 15, [...]).

Ponadto niektóre zastosowane sformułowania, np. „uzgodniony z klientem” (s. 10), „klienci muszą mieć możliwość wyboru” (s. 11), można by połączyć z koniecznością uzyskania „zgody”, jak określono w art. 2 lit. h) dyrektywy.

Grupa Robocza Art. 29 wnosi również o rozważenie wskazania stosownej terminologii dotyczącej ochrony danych oraz o wyjaśnienie w stosownych przypadkach poziomu interoperacyjności terminów.

2.7 Wnioski i zalecenia

Grupa Robocza Art. 29 dostrzega prace przeprowadzone przez grupę EG2 i zdaje sobie sprawę z tego, że druga wersja szablonu jest znacznie lepsza od poprzedniej wersji pod tym względem, że metodyka jest lepiej przedstawiona i łatwiejsza do wykonania. Nadal jednak istnieje szereg niejasnych elementów i potrzeba większej przejrzystości w określonych częściach, które - jeśli zostaną poprawione we wskazany sposób - przyczynią się w decydujący sposób do pomyślnego wdrożenia i stosowania szablonu.

Grupa Robocza Art. 29 rozumie, że wersja, którą oceniła, wciąż może zostać poddana redakcji językowej i prawnej.

Grupa Robocza Art. 29 zdaje sobie sprawę, że sektor przemysłu pilnie potrzebuje oceny skutków w zakresie ochrony danych, i z zadowoleniem przyjmuje szybko opracowaną ostateczną wersję szablonu, którego skuteczność z pewnością trzeba będzie zweryfikować i poprawić po pewnym okresie stosowania. Grupa Robocza Art. 29 zaleca w związku z tym zorganizowanie etapu testowego z pewnymi prawdziwymi przypadkami, o którym należy ją poinformować i w ramach którego poszczególne organy ochrony danych mogą rozważyć zaoferowanie wsparcia. Etap ten powinien również przyczynić się do zagwarantowania, że szablon zapewnia osobom fizycznym lepszą ochronę danych w kontekście wprowadzania inteligentnych sieci. Podczas testowania szablonu oraz zgodnie z tym, co w nim przewidziano, zachęca się sektor przemysłu do zwrócenia uwagi na najważniejsze pojęcia związane z reformą ochrony

danych, takie jak: uwzględnienie ochrony danych już w fazie projektowania, domyślna ochrona danych, minimalizacja danych, prawo do bycia zapomnianym i możliwość przenoszenia danych.

Ponadto Grupa Robocza Art. 29 nadal zaleca rozważenie możliwości określenia ogólnej metodyki dokonywania oceny skutków w zakresie ochrony danych, która mogłaby być przydatna w pracach związanych z poszczególnymi obszarami.

Sporządzono w Brukseli dnia 4 grudnia 2013 r.

W imieniu Grupy Roboczej
Przewodniczący
Jacob KOHNSTAMM

Załącznik: Dodatkowe narzędzia metodologiczne

W sekcji „3.5. Etap 5 – Ocena ryzyka dla ochrony danych” można by wykorzystać poniższą tabelę do oceny zdarzeń, co do których istnieją obawy:

Przetwarzanie i dane osobowe	Poziom identyfikacji (LI)	Zdarzenia, co do których istnieją obawy	Potencjalne skutki	Negatywne skutki (PE)	Powaga (LI+PE)
[wykaz danych osobowych objętych przetwarzaniem]	[najodpowiedniejszy poziom w skali poziomu identyfikacji, na podstawie danych osobowych]	[zdarzenie, co do którego istnieją obawy]	[wykaz potencjalnych konsekwencji dla osób, których dane dotyczą, w przypadku zaistnienia zdarzenia, co do którego istnieją obawy]	[najodpowiedniejszy poziom w skali negatywnych skutków, na podstawie potencjalnych skutków]	[zwiększenie]

Jeżeli dane osobowe nie są oceniane całościowo, wiersze te należy powtórzyć (np. dla każdego procesu).

Samą tabelę można powiększyć o dalsze kolumny odpowiadające zagrożeniom, tak aby można było ukazać całe ryzyko:

Przetwarzanie i dane osobowe	Poziom identyfikacji (LI)	Zdarzenia co do których istnieją obawy	Potencjalne skutki	Negatywne skutki (PE)	Powaga (LI+PE)	Główne zagrożenia	Słabe strony (VUL)	Źródła ryzyka	Zdolności (CAP)	Prawdopodobieństwo (VUL+ CAP)

Należy dodać nową sekcję, aby wykazać zgodność z celami w zakresie ochrony prywatności. Sekcja ta mogłaby znajdować się pomiędzy sekcjami 2.6.2 i 2.6.3 i być zatytułowana „2.6.3. Zgodność z celami w zakresie ochrony prywatności”. Ponieważ te cele w zakresie ochrony prywatności są obowiązkowe i nie podlegają negocjacji, w sekcji tej należy wskazać, że w odniesieniu do każdego z celów w zakresie ochrony

prywatności należy opisać sposób jego realizacji lub podać uzasadnienie niezrealizowania tego celu[9].

W tym celu można wykorzystać poniższą tabelę:

Cele w zakresie ochrony prywatności	Wyjaśnienia	Opis/ uzasadnienie
Zabezpieczenie jakości danych osobowych	Najważniejsze cele, które należy być zapewnić, to: unikanie i minimalizacja danych, określanie i ograniczenie celu oraz jakość i przejrzystość danych.	[opis sposobu, w jaki zrealizowano cel w zakresie ochrony prywatności, LUB uzasadnienie, jeżeli nie zrealizowano tego celu]
Zasadność przetwarzania danych osobowych	Zasadność przetwarzania danych osobowych należy zapewnić poprzez oparcie przetwarzania danych na wyraźnej zgodzie, umowie, obowiązku prawnym itp.	[opis sposobu, w jaki zrealizowano cel w zakresie ochrony prywatności, LUB uzasadnienie, jeżeli nie zrealizowano tego celu]
Zasadność przetwarzania szczególnie chronionych danych osobowych	Zasadność przetwarzania szczególnie chronionych danych osobowych należy zapewnić poprzez oparcie przetwarzania danych na wyraźnej zgodzie, szczególnej podstawie prawnej itp.	[opis sposobu, w jaki zrealizowano cel w zakresie ochrony prywatności, LUB uzasadnienie, jeżeli nie zrealizowano tego celu]
Przestrzeganie prawa osoby, której dane dotyczą, do informacji	Należy zapewnić poinformowanie w odpowiednim czasie, osoby, której dane dotyczą, o gromadzeniu jej danych.	[opis sposobu, w jaki zrealizowano cel w zakresie ochrony prywatności, LUB uzasadnienie, jeżeli nie zrealizowano tego celu]
Przestrzeganie prawa osoby, której dane dotyczą, do dostępu do danych oraz do ich poprawienia i usunięcia	Należy zapewnić zrealizowanie w odpowiednim czasie życzenia osoby, której dane dotyczą, w odniesieniu do dostępu do jej danych oraz ich poprawienia, usunięcia i zablokowania. Należy zachęcać do wdrożenia prawa do bycia zapomnianym i prawa do możliwości przeniesienia danych	[opis sposobu, w jaki zrealizowano cel w zakresie ochrony prywatności, LUB uzasadnienie, jeżeli nie zrealizowano tego celu]
Przestrzeganie prawa wniesienia sprzeciwu przez osobę, której dane dotyczą	Należy zagwarantować, że jeżeli osoba, której dane dotyczą, wniesie sprzeciw, jej dane nie będą dalej przetwarzane. Przejrzystość zautomatyzowanych decyzji dotyczących osób fizycznych musi być zapewniona w szczególności w przypadku profilowania.	[opis sposobu, w jaki zrealizowano cel w zakresie ochrony prywatności, LUB uzasadnienie, jeżeli nie zrealizowano tego celu]
Zabezpieczenie poufności i bezpieczeństwa przetwarzania danych	Najważniejsze cele, które należy zapewnić, to: zapobieganie nieuprawnionemu dostępowi, rejestrowanie przetwarzania danych, bezpieczeństwo sieci i transportu oraz zapobieganie przypadkowej utracie danych. Należy promować procedurę zawiadamiania o naruszeniu ochrony danych.	[opis sposobu, w jaki zrealizowano cel w zakresie ochrony prywatności, LUB uzasadnienie, jeżeli nie zrealizowano tego celu]
Przestrzeganie wymogów dotyczących zawiadamiania	Najważniejsze cele, które należy zapewnić, to zawiadamianie o przetwarzaniu danych, wstępna kontrola zgodności i dokumentacja. W odniesieniu do tego celu ocenę skutków w zakresie ochrony danych uznaje się za narzędzie wyznaczające.	[opis sposobu, w jaki zrealizowano cel w zakresie ochrony prywatności, LUB uzasadnienie, jeżeli nie zrealizowano tego celu]

[9] Jest to porównywalne z pojęciem „deklaracji stosowania” zawartym w normie ISO/IEC 27001.

Cele w zakresie ochrony prywatności	Wyjaśnienia	Opis/ uzasadnienie
Przestrzeganie wymogów dotyczących zatrzymywania danych	Dane powinny być zatrzymywane na minimalny okres zgodny z celem zatrzymywania lub innymi wymogami prawnymi.	[opis sposobu, w jaki zrealizowano cel w zakresie ochrony prywatności, LUB uzasadnienie, jeżeli nie zrealizowano tego celu]
Uwzględnienie ochrony prywatności już w fazie projektowania	Zaprojektowanie środków i procedur technicznych i organizacyjnych, z uwzględnieniem najnowszych osiągnięć technicznych oraz kosztów wdrożenia, zarówno w momencie ustalania środków niezbędnych do przetwarzania, jak i w momencie samego przetwarzania, w taki sposób, aby te środki i procedury w pełni przestrzegały prawa osoby, której dane dotyczą, do ochrony prywatności i danych.	[opis sposobu, w jaki zrealizowano cel w zakresie ochrony prywatności, LUB uzasadnienie, jeżeli nie zrealizowano tego celu]
Domyślna ochrona prywatności	Należy wdrożyć mechanizmy służące zagwarantowaniu, by domyślnie przetwarzane były jedynie te dane osobowe, które są niezbędne dla realizacji każdorazowego szczególnego celu przetwarzania, oraz by w szczególności nie były one gromadzone lub zatrzymywane dłużej niż przez minimalny okres niezbędny do realizacji tych celów, zarówno jeśli chodzi o ilość danych, jak i okres ich przechowywania.	[opis sposobu, w jaki zrealizowano cel w zakresie ochrony prywatności, LUB uzasadnienie, jeżeli nie zrealizowano tego celu]

Oczywiście każdą z wyżej wymienionych pozycji można zwielokrotnić, aby dodatkowo podzielić każdy cel w zakresie ochrony prywatności, jeśli jest to użyteczne. Na przykład „jakość danych" obejmuje wiele innych zasad, takich jak unikanie i minimalizacja danych, konieczność i proporcjonalność w odniesieniu do celów itp. Ponadto zasadne może być ujęcie różnych środków kontroli stosowanych na potrzeby zrealizowania tego samego celu w zakresie ochrony prywatności w odrębnych pozycjach, aby wyróżnić te środki.

W ten sposób zarządza się zatem ryzykiem w zakresie ochrony danych (ocenia i odpowiednio je traktuje) oraz opisuje (i można kontrolować) działania podejmowane na potrzeby zrealizowania celów w zakresie ochrony prywatności.

Nadal możliwe jest zastosowanie podejścia mieszanego poprzez przeanalizowanie także ryzyka pominięcia niektórych celów w zakresie ochrony prywatności (nie tylko bezpieczeństwa, ale także np. ograniczania celu, konieczności i proporcjonalności, zatrzymywania danych, przyznania praw osobom, których dane dotyczą, itp.).