OCENA SKUTKÓW PRZEDSIĘWZIĘCIA DLA OCHRONY PRYWATNOŚCI (Privacy Impact Assessment) W SEKTORZE UBEZPIECZENIOWYM

XII edycja seminarium Polskiej Izby Ubezpieczeo

„Jakośd danych w systemach informatycznych zakładów ubezpieczeo”

DR WOJCIECH WIEWIÓROWSKI
Wydział Prawa i Administracji Uniwersytetu Gdańskiego
Generalny Inspektor Ochrony Danych Osobowych

18 października 2012 r.
Warszawa

Generalny Inspektor
Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa
www.giodo.gov.pl
kancelaria@giodo.gov.pl

TEMATYKA WYKŁADU

1. Ocena wpływu na prywatność – Privacy Impact Assessment (PIA)
2. Profilowanie – zasady ogólne
3. Reforma prawa ochrony danych osobowych w Unii Europejskiej
4. Regulacja „ryzykownego przetwarzania danych” oraz PIA
5. Rola samoregulacji
6. Jak tworzona jest ocena wpływu przedsięwzięcia na ochronę danych osobowych
7. Zalecane PIA sektorowe na przykładzie RFID
8. Ochrona prywatności w fazie projektowania (privacy by design)

KONSTYTUCJA RZECZYPOSPOLITEJ POLSKIEJ (art. 47)

Każdy ma prawo do ochrony życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.

KONSTYTUCJA RZECZYPOSPOLITEJ POLSKIEJ (art. 51)

1. *Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby.*
2. *Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.*
3. *Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa.*
4. *Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.*
5. *Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.*

OCENA WPŁYWU NA PRYWATNOŚĆ
Privacy Impact Assessment - PIA

- Ocena skutków przedsięwzięcia dla prywatności (*privacy impact assessment, PIA*), jako sposób realizacji zasad prywatności na etapie projektowania i realizacji projektu (*privacy by design*, PbD).
- PbD zakłada, że podmiot tworzący rozwiązanie organizacyjne lub techniczne powinien na każdym etapie projektowania i realizacji projektu wykazać proaktywne - nie reaktywne, zaradcze - nie naprawcze podejście do zagadnień prywatności. Powinien przyjąć, że jego system będzie z zasady chronił prywatność (*privacy by default*). Zasady ochrony prywatności powinny być immanentnie włączone w projekt i respektowane przez twórców i użytkowników od początku do końca cyklu życia informacji. Jednocześnie wykonanie obowiązku informacyjnego wobec osoby, której dane dotyczą jest niczym innym niż realizacją transparentności i przejrzystości oraz poszanowania dla prywatności użytkowników.
- Koncept PIA w sposób naturalny uzupełnia i daje praktyczny wymiar *privacy by design*. Patrząc na projekt nowych ram prawnych ochrony danych osobowych przedstawiony przez Komisję Europejską na początku 2012 r., należy stwierdzić, że zarówno prywatność na etapie projektowania, jak i ocena wpływu przedsięwzięcia na ochronę prywatności znalazły w tychże ramach swoje poczesne miejsce. Co ciekawe, dotyczy to generalnego rozporządzenia o ochronie danych osobowych, jak również dyrektywy, która ma obowiązywać w dawnym III filarze Unii Europejskiej.

OCENA WPŁYWU NA PRYWATNOŚĆ
Privacy Impact Assessment - PIA

- Projekt nowych ram prawnych ochrony danych w Unii Europejskiej stawia już znacznie więcej wymagań, jeśli chodzi o stosowanie PIA. Komisja, decydując się na odejście od notyfikacji i rejestracji zbiorów jako zasady, zastępuje ją obowiązkiem przeprowadzania oceny skutków przetwarzania danych dla ochrony prywatności osób fizycznych. Komisja nie określa, na czym dokładnie ma polegać ocena – wydaje się, że wciąż czeka na propozycje takich testów, które powstają obecnie w środowisku naukowym – ale stwierdza, że wyniki takiej oceny powinny być z zasady (choć dopuszczane są tu wyjątki) dostępne publicznie, a oceną należy objąć przede wszystkim przewidywane środki, mechanizmy i zabezpieczenia, które powinny prowadzić do zgodności przetwarzania danych z wymaganiami prawa europejskiego.

OCENA WPŁYWU NA PRYWATNOŚĆ
Privacy Impact Assessment - PIA

- Szczególną rolę PIA spełniał będzie wtedy, gdy jego wyniki będą wskazywać, że przetwarzanie danych w ramach danego projektu może rodzić „wysoki stopień szczególnego ryzyka dla praw i wolności osoby” (*involves a high degree of specific risks to the rights and freedoms of data subjects*). Stanie się on bowiem podstawą do oceny projektu przez organ ochrony danych osobowych (w Polsce przez GIODO). Jest tym samym oczywiste, że tego typu ocena musi się pojawić na etapie projektowania. Jej wynik bowiem doprowadzi dopiero do decyzji, czy przetwarzanie danych w projektowany sposób musi podlegać uprzedniej konsultacji i aprobacie ze strony rzecznika ochrony danych osobowych. Co jednak ciekawe, w art. 30 proponowanego rozporządzenia Komisja podjęła się wymienienia operacji na danych osobowych, które jej zdaniem mogą powodować powstanie takiego realnego zagrożenia dla praw i wolności osób.

OCENA WPŁYWU NA PRYWATNOŚĆ
Privacy Impact Assessment - PIA

Za operacje takie uznano:

- profilowanie – opisane jako: ocena, analiza lub przewidywanie aspektów osobowych w stosunku do osób fizycznych w zakresie zachowania w pracy, zdolności kredytowej (*creditworthiness*), sytuacji ekonomicznej, lokalizacji, zdrowia, osobistych preferencji, wiarygodności (*reliability*) lub zachowania, jeśli takie przewidywanie oparte jest na automatycznym przetwarzaniu danych i może wpływać znacząco na sytuacje osoby;
- przetwarzanie danych o życiu seksualnym, zdrowiu, pochodzeniu rasowym i etnicznym lub (co można określić jako nową listę danych wrażliwych);
- przetwarzanie danych osobowych na potrzeby ochrony zdrowia, badań epidemiologicznych lub badań nad chorobami psychicznymi lub zakaźnymi;
- monitorowanie publicznie dostępnych miejsc, a w szczególności wideo nadzór;
- przetwarzanie w systemach wielkoskalowych danych osobowych dzieci, danych biometrycznych lub genetycznych.

OCENA WPŁYWU NA PRYWATNOŚĆ
Privacy Impact Assessment - PIA

- Jednocześnie projektodawcy zwracają uwagę (art. 30 ust. 4) na konieczność konsultowania zamiaru przetwarzania danych osobowych z pomiotami, których dane mają być przetwarzane, lub z ich przedstawicielami. Nie wyjaśniono w żaden sposób, na czym tego typu konsultacja miałaby polegać, ale widać w tej idei wpływ prawa ochrony konsumentów, gdzie rola stowarzyszeń konsumenckich przy tego typu działaniach jest już od dawna uznawana za oczywistą.
- Warto zwrócić uwagę, że przetwarzanie danych na potrzeby ochrony zdrowia (*for the provison of health care*) odróżniane jest wyraźnie od przetwarzania danych „o zdrowiu”. Ten pierwszy termin ma więc zdaniem projektodawców znacznie szersze znaczenie. Można uznać, że w tym przypadku chodzi o przetwarzanie jakichkolwiek danych osobowych w systemach używanych w ochronie zdrowia, które w jakikolwiek sposób (automatycznie lub manualnie) mogłyby być łączone z danymi osobowymi pacjentów, lekarzy, personelu medycznego i pomocniczego. W każdym takim przypadku należy przygotować ocenę skutków projektu dla ochrony prywatności i aktualizować takie PIA na każdym etapie tworzenia systemu.

OCENA WPŁYWU NA PRYWATNOŚĆ
Privacy Impact Assessment - PIA

- A ***Privacy Impact Assessment (PIA) is a process whereby a conscious and*** systematic effort is made to assess the privacy and data protection impacts of a specific technology with the view of taking appropriate actions to prevent or at least minimise those impacts.
- The ***Framework identifies the objectives of PIAs, the components*** of enterprise to be considered during PIAs, and the common structure and content of RFID Application PIA Reports.
- A ***PIA Report is the document resulting from the PIA Process that is made available*** to competent authorities. Proprietary and security sensitive information may be removed from PIA Reports before the Reports are provided externally (e.g., to the competent authorities) as long as the information is not specifically pertinent to privacy and data protection implications. The manner in which the PIA should be made available (e.g., upon request or not) will be determined by member states. In particular, the use of special categories of data may be taken into account, as well as other factors such as the presence of a data protection officer.
- ***PIA Templates may be developed based on the Framework to provide industrybased,*** application-based, or other specific formats for PIAs and resulting PIA Reports.

OCENA SKUTKÓW W ZAKRESIE OCHRONY DANYCH W PROJEKCIE NOWYCH RAM OCHRONY DANYCH W UE

Artykuł 33 ***Ocena skutków w zakresie ochrony danych***

1. Jeśli operacje przetwarzania stwarzają szczególne ryzyko dla praw i wolności podmiotów danych z racji swego charakteru, zakresu lub celów, administrator lub podmiot przetwarzający przeprowadzają w imieniu administratora danych ocenę skutków przewidywanych operacji przetwarzania w zakresie ochrony danych osobowych.

OCENA SKUTKÓW W ZAKRESIE OCHRONY DANYCH W PROJEKCIE NOWYCH RAM OCHRONY DANYCH W UE

Artykuł 33 (…)

2. **Szczególne ryzyko**, o którym mowa w ust. 1, **stwarzają w szczególności** następujące operacje przetwarzania:

a) systematyczna i kompleksowa ocena aspektów osobowych osoby fizycznej bądź operacje przetwarzania mające na celu analizę lub przewidzenie w szczególności **sytuacji ekonomicznej, miejsca pobytu, stanu zdrowia, preferencji osobistych, wiarygodności lub zachowania osoby fizycznej**, która opiera się na automatycznym przetwarzaniu, i na której opierają się środki, które wywołują skutki prawne dotyczące danej osoby lub mają na nią istotny wpływ;

b) przetwarzanie informacji na temat życia seksualnego, stanu zdrowia, rasy i pochodzenia etnicznego oraz świadczenia usług opieki zdrowotnej, badań epidemiologicznych lub badań mających na celu wykrycie chorób psychicznych bądź zakaźnych, **jeśli dane są przetwarzane w celu podjęcia na szeroką skalę środków lub decyzji dotyczących konkretnych osób**;

c) monitorowanie publicznie dostępnych miejsc, zwłaszcza przy wykorzystaniu urządzeń optyczno-elektronicznych (wideonadzór) na szeroką skalę;

d) przetwarzanie danych osobowych w wielkoskalowych zbiorach danych dotyczących dzieci, danych genetycznych lub biometrycznych; (…)

NARUSZENIE OCHRONY DANYCH OSOBOWYCH

„naruszenie ochrony danych osobowych” oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub dostępu do danych osobowych przesyłanych, przechowywanych lub przetwarzanych w inny sposób;

NARUSZENIE OCHRONY DANYCH OSOBOWYCH ROZPORZĄDZENIE

Artykuł 31 ***Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu***

1. W przypadku naruszenia ochrony danych osobowych, administrator zgłasza organowi nadzorczemu takie naruszeniu bez nieuzasadnionej zwłoki i jeśli jest to możliwe, nie później niż w ciągu 24 godzin od momentu dowiedzenia się o tym naruszeniu. Jeśli organ nadzorczy nie zostanie zawiadomiony w ciągu 24 godzin, do zgłoszenia należy dołączyć umotywowane wyjaśnienie. (…)

3. Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:

a) opisywać charakter naruszenia ochrony danych osobowych, w tym podawać kategorie i liczbę zainteresowanych podmiotów danych oraz kategorie i liczbę rekordów danych, których dotyczy naruszenie;

b) podawać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub innego punktu kontaktowego, w którym można uzyskać więcej informacji;

c) zalecać środki mające na celu zmniejszenie ewentualnych negatywnych skutków naruszenia ochrony danych osobowych;

d) opisywać konsekwencje naruszenia ochrony danych;

e) opisywać środki proponowane lub podjęte przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych.

NARUSZENIE OCHRONY DANYCH OSOBOWYCH ROZPORZĄDZENIE

Artykuł 31 ***Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu***
(…).
4. Administrator sporządza dokumentację dotyczącą wszelkich naruszeń ochrony danych osobowych, obejmującą okoliczności naruszenia, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi umożliwiać organowi nadzorczemu sprawdzenie zgodności z niniejszym artykułem. Dokumentacja zawiera wyłącznie informacje niezbędne do realizacji powyższego celu.
5. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 86 w celu doprecyzowania kryteriów i wymogów dotyczących stwierdzenia naruszenia ochrony danych osobowych, o którym mowa w ust. 1 i 2, oraz szczególnych okoliczności, w których administrator i podmiot przetwarzający mają obowiązek zgłosić naruszenie ochrony danych osobowych.
6. Komisja może ustanowić standardowe formularze zgłoszenia przekazywanego organowi nadzorczemu, procedury mające zastosowanie do wymogu zgłoszenia, a także formę i sposób prowadzenia dokumentacji, o której mowa w art. 4, w tym terminy usuwania zawartych w niej informacji. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 87 ust. 2.

NARUSZENIE OCHRONY DANYCH OSOBOWYCH ROZPORZĄDZENIE

Artykuł 32 ***Zawiadomienie podmiotu danych o naruszeniu ochrony danych osobowych***

1. Gdy istnieje prawdopodobieństwo, że naruszenie ochrony danych osobowych może niekorzystnie wpłynąć na ochronę danych osobowych lub prywatność podmiotu danych, administrator, po dokonaniu zgłoszenia, o którym mowa w art. 31, bez nieuzasadnionej zwłoki informuje podmiot danych o naruszeniu ochrony danych osobowych.
2. Zawiadomienie przekazane podmiotowi danych, o którym mowa w ust. 1, opisuje charakter naruszenia ochrony danych osobowych i zawiera przynajmniej informacje i zalecenia, o których mowa w art. 31 ust. 3 lit. b) i c).
3. Zawiadomienie podmiotu danych o naruszeniu ochrony danych osobowych nie jest wymagane, jeśli administrator wykaże, zgodnie z wymogami organu nadzorczego, że wdrożył odpowiednie technologiczne środki ochrony oraz że środki te zostały zastosowane do danych, których dotyczyło naruszenie ochrony danych osobowych. Tego rodzaju technologiczne środki ochrony sprawiają, że dane stają się nieczytelne dla każdego, kto nie jest uprawniony do dostępu do nich.
4. Bez uszczerbku dla obowiązku administratora w zakresie zawiadomienia podmiotu danych o naruszeniu ochrony danych osobowych, jeśli administrator nie zawiadomił wcześniej podmiotu danych o naruszeniu ochrony danych osobowych, organ nadzorczy może tego od niego zażądać, jeśli stwierdzi możliwość wystąpienia niekorzystnych skutków naruszenia.

NARUSZENIE OCHRONY DANYCH OSOBOWYCH DYREKTYWA

Artykuł 28 ***Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu***

1. Państwa członkowskie stanowią przepisy przewidujące, że w przypadku naruszenia ochrony danych osobowych, administrator zgłasza organowi nadzorczemu takie naruszenie bez nieuzasadnionej zwłoki i, w jeśli to możliwe, nie później niż w ciągu 24 godzin od momentu dowiedzenia się o tym naruszeniu. Na żądanie organu nadzorczego administrator dostarcza umotywowane wyjaśnienie w przypadkach, w których zgłoszenie nie zostało przekazane w ciągu 24 godzin. (…)
3. Zgłoszenie, o którym mowa w ust. 1, zawiera co najmniej:
   a) opis charakteru naruszenia ochrony danych osobowych, w tym kategorie i liczbę zainteresowanych podmiotów danych oraz kategorie i liczbę rekordów danych, których dotyczy naruszenie;
   b) imię i nazwisko oraz dane kontaktowe inspektora ochrony danych, o którym mowa w art. 30, lub innego punktu kontaktowego, w którym można uzyskać więcej informacji;
   c) zalecenia dotyczące środków mające na celu zmniejszenie ewentualnych negatywnych skutków naruszenia ochrony danych osobowych;
   d) opis potencjalnych konsekwencji naruszenia ochrony danych osobowych;
   e) opis środków proponowanych lub podjętych przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych.

NARUSZENIE OCHRONY DANYCH OSOBOWYCH DYREKTYWA

Artykuł 28 ***Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu***

4. Państwa członkowskie stanowią przepisy przewidujące, że administrator sporządza dokumentację dotyczącą wszelkich naruszeń ochrony danych osobowych, obejmującą okoliczności naruszenia, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi umożliwiać organowi nadzorczemu sprawdzenie zgodności z niniejszym artykułem. Dokumentacja zawiera wyłącznie informacje niezbędne do realizacji powyższego celu.
5. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 56 w celu doprecyzowania kryteriów i wymogów dotyczących stwierdzenia naruszenia ochrony danych osobowych, o którym mowa w ust. 1 i 2, oraz szczególnych okoliczności, w których administrator i podmiot przetwarzający mają obowiązek zawiadomić o naruszeniu ochrony danych osobowych.
6. Komisja może ustanowić standardowe formularze zawiadomienia przekazywanego organowi nadzorczemu, procedury mające zastosowanie do wymogu zawiadomienia, a także formę i sposób prowadzenia dokumentacji, o której mowa w art. 4, w tym terminy usuwania zawartych w niej informacji. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 57 ust. 2.

NARUSZENIE OCHRONY DANYCH OSOBOWYCH DYREKTYWA

Artykuł 29 ***Zawiadomienie podmiotu danych o naruszeniu ochrony danych osobowych***

1. Państwa członkowskie stanowią przepisy przewidujące, że gdy istnieje prawdopodobieństwo, że naruszenie ochrony danych osobowych może niekorzystnie wpłynąć na ochronę danych osobowych lub prywatność osoby, administrator, po dokonaniu zawiadomienia, o którym mowa w art. 28, bez nieuzasadnionej zwłoki informuje podmiot danych o naruszeniu ochrony danych osobowych.
2. Zawiadomienie przekazane podmiotowi danych, o którym mowa w ust. 1, opisuje charakter naruszenia ochrony danych osobowych i zawiera przynajmniej informacje i zalecenia, o których mowa w art. 28 ust. 3 lit. b) i c).
3. Zawiadomienie o naruszeniu ochrony danych osobowych nie jest wymagane, jeśli administrator wykaże, zgodnie z wymogami organu nadzorczego, że wdrożył odpowiednie technologiczne środki ochrony oraz że środki te zostały zastosowane do danych, których dotyczyło naruszenie ochrony danych osobowych. Tego rodzaju technologiczne środki ochrony sprawiają, że dane stają się nieczytelne dla każdego, kto nie jest uprawniony do dostępu do nich.
4. Zawiadomienie podmiotu danych może zostać opóźnione, ograniczone lub zaniechane z przyczyn, o których mowa w art. 11 ust. 4.

OCENA SKUTKÓW W ZAKRESIE OCHRONY DANYCH OSOBOWYCH NA PRZYKŁADZIE PIA DLA RFID

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

I. **fazę oceny wstępnej**, w ramach której dokonuje się klasyfikacji zastosowanych działań według czterostopniowej skali na podstawie schematu podejmowania decyzji. Wynik tej oceny pozwala ustalić, czy ocena skutków w zakresie ochrony danych i prywatności jest potrzebna oraz dokonać wyboru między „pełną oceną skutków w zakresie ochrony danych i prywatności" a „niepełną oceną skutków w zakresie ochrony danych i prywatności". Zastosowania, w których wykorzystuje się identyfikatory, które przypuszczalnie będą dotyczyły osób fizycznych, będą wymagać przeprowadzenia co najmniej „niepełnej oceny skutków w zakresie ochrony danych i prywatności" (poziom 1), zaś zastosowania, w ramach których dokonuje się dalszego przetwarzania danych osobowych będą wymagać przeprowadzenia „pełnej oceny skutków w zakresie ochrony danych i prywatności" (poziom 2 i 3). Odwrotnie, zastosowania w których nie wykorzystuje się identyfikatorów noszonych przez osoby fizyczne i w ramach których nie ma dalszego przetwarzania danych osobowych, nie podlegają ocenie skutków w zakresie ochrony danych i prywatności (poziom 0).

OCENA SKUTKÓW W ZAKRESIE OCHRONY DANYCH OSOBOWYCH NA PRZYKŁADZIE PIA DLA RFID

II. faza oceny ryzyka, która dzieli się na **cztery główne etapy**:

1) ***charakterystyka zastosowania*** (rodzaje danych, przepływy danych, technologia, przechowywanie i transfery danych itp.);
2) **identyfikacja rodzajów ryzyka** związanego z danymi osobowymi poprzez ocenę zagrożeń, prawdopodobieństwa ich wystąpienia oraz wpływu, jeśli chodzi o prywatność i zgodność z prawodawstwem europejskim;
3) **określenie rodzajów kontroli** oraz **sformułowanie zaleceń** dotyczących ich przeprowadzania, jako odpowiedź na uprzednio zidentyfikowane rodzaje ryzyka;
4) **udokumentowanie wyników oceny** skutków w zakresie ochrony danych i prywatności, znalezienie rozwiązania dotyczącego warunków wdrożenia ocenianego zastosowania oraz informowanie o pozostałym ryzyku.

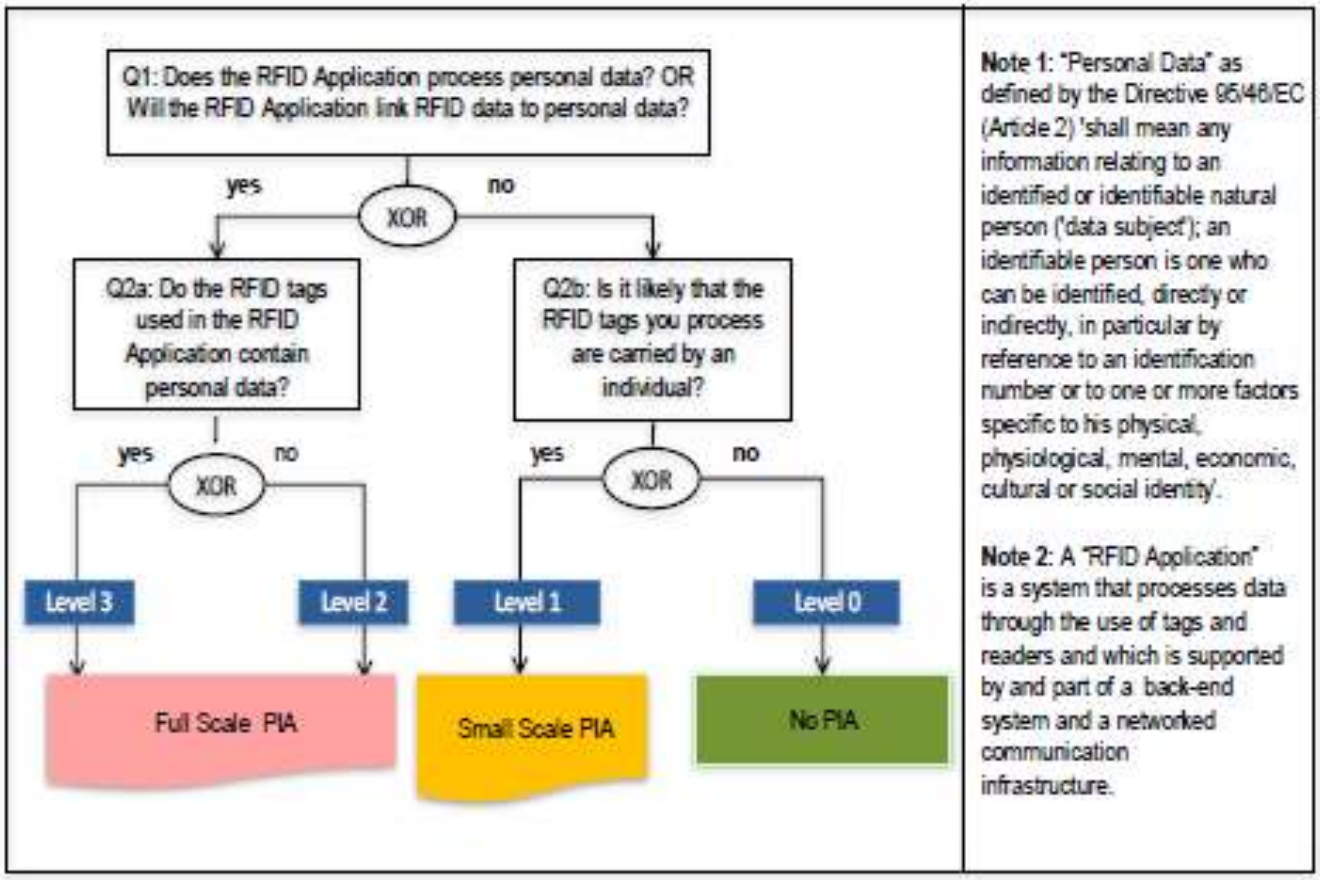
OCENA SKUTKÓW W ZAKRESIE OCHRONY DANYCH OSOBOWYCH NA PRZYKŁADZIE PIA DLA RFID

Na każdym etapie fazy oceny ryzyka organy regulacyjne i środowiska samoregulacyjne powinny zapewnić dodatkowe wsparcie w postaci wskazówek dla osoby przeprowadzającej ocenę. Należą do nich:

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

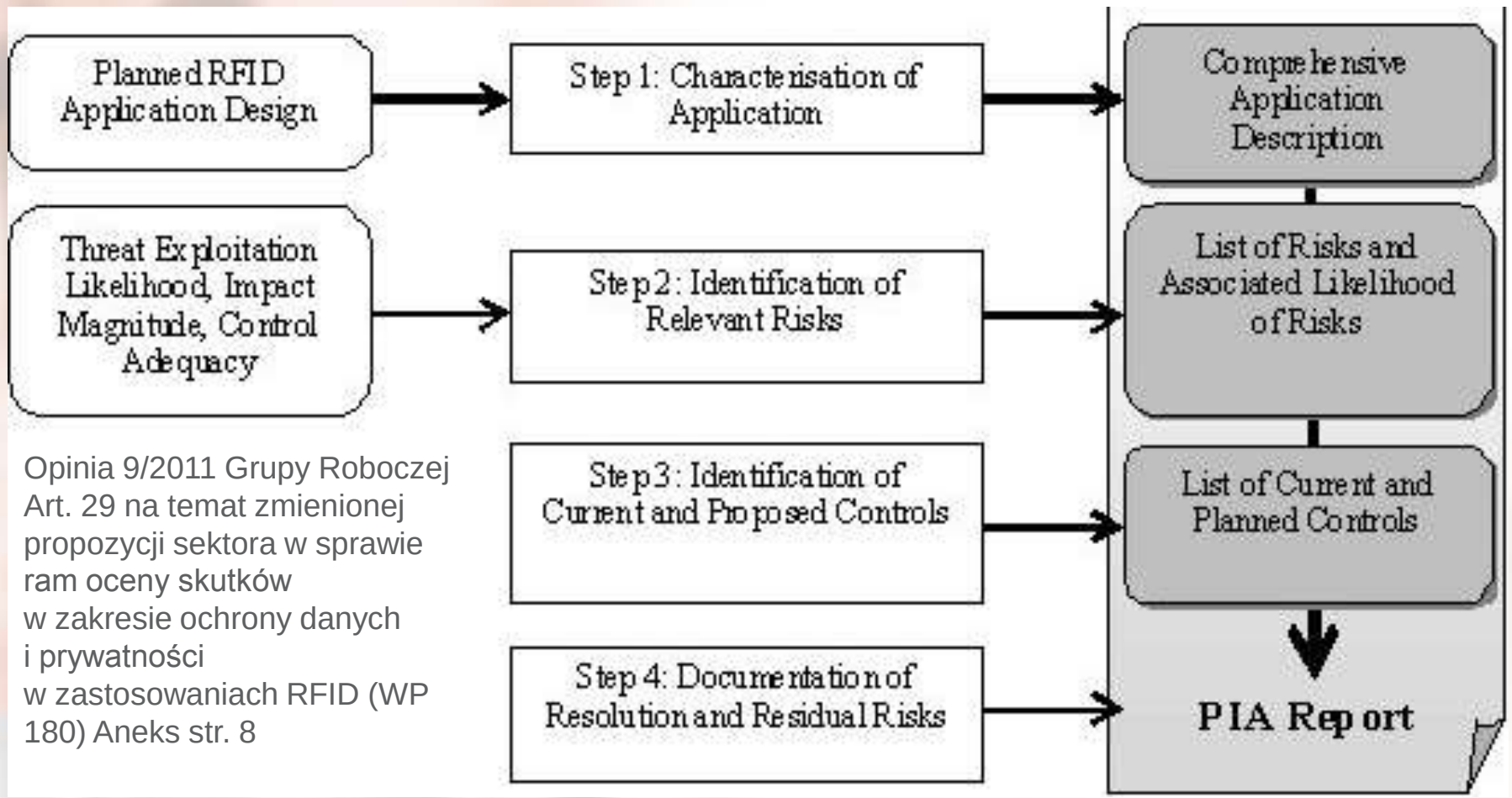
Wynik oceny skutków w zakresie ochrony danych i prywatności przyjmuje oficjalną formę sprawozdania z oceny skutków w zakresie ochrony danych i prywatności, przygotowanego przez podejmującego działanie, które zawiera opis przedsięwzięcia oraz dokumentuje szczegóły wspomnianych powyżej czterech etapów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

OCENA SKUTKÓW W ZAKRESIE OCHRONY DANYCH OSOBOWYCH NA PRZYKŁADZIE PIA DLA RFID



Decision Tree on whether and at what level of detail to conduct a PIA, Opinia 9/2011 Grupy Roboczej Art. 29 na temat zmienionej propozycji sektora w sprawie ram oceny skutków w zakresie ochrony danych i prywatności w zastosowaniach RFID (WP 180) Aneks str. 7

OCENA SKUTKÓW W ZAKRESIE OCHRONY DANYCH OSOBOWYCH NA PRZYKŁADZIE PIA DLA RFID



Opinia 9/2011 Grupy Roboczej Art. 29 na temat zmienionej propozycji sektora w sprawie ram oceny skutków w zakresie ochrony danych i prywatności w zastosowaniach RFID (WP 180) Aneks str. 8

OCENA SKUTKÓW W ZAKRESIE OCHRONY DANYCH OSOBOWYCH NA PRZYKŁADZIE PIA DLA RFID

Na podst. opinii 9/2011 Gr. Roboczej Art. 29 nt. zmienionej propozycji sektora w sprawie ram oceny skutków w zakresie ochrony danych i prywatności w zastosowaniach RFID (WP 180) Aneks II

ANNEX II - *Privacy Targets (…)*

1. ***Safeguarding quality of personal data***
   Data avoidance and minimisation, purpose specification and limitation, quality of data and transparency are the key targets that need to be ensured.
2. ***Legitimacy of processing personal data***
   Legitimacy of processing personal data must be ensured either by basing data processing on consent, contract, legal obligation, etc.
3. ***Legitimacy of processing sensitive personal data***
   Legitimacy of processing sensitive personal data must be ensured either by basing data processing on explicit consent, a special legal basis, etc.
4. ***Compliance with the data subject's right to be informed***
   It must be ensured that the data subject is informed about the collection of his data in a timely manner.
5. ***Compliance with the data subject's right of access to data, correct and erase data***
   It must be ensured that the data subject's wish to access, correct, erase and block his data is fulfilled in a timely manner.

OCENA SKUTKÓW W ZAKRESIE OCHRONY DANYCH OSOBOWYCH NA PRZYKŁADZIE PIA DLA RFID

Na podst. opinii 9/2011 Gr. Roboczej Art. 29 nt. zmienionej propozycji sektora w sprawie ram oceny skutków w zakresie ochrony danych i prywatności w zastosowaniach RFID (WP 180) Aneks II

ANNEX II - *Privacy Targets (…)*

6. ***Compliance with the data subject's right to object***
   It must be ensured that the data subject's data is no longer processed if he or she objects. Transparency of automated decisions vis-à-vis individuals must be ensured especially.
7. ***Safeguarding confidentiality and security of processing***
   Preventing unauthorised access, logging of data processing, network and transport security and preventing accidental loss of data are the key targets that need to be ensured.
8. ***Compliance with notification requirement***
   Notification about data processing, prior compliance checking and documentation are the key targets that need to be ensured.
9. **Compliance with data retention requirements**
   Retention of data should be for the minimum period of time consistent with the purpose of the retention or other legal requirements.

OCENA SKUTKÓW W ZAKRESIE OCHRONY DANYCH OSOBOWYCH NA PRZYKŁADZIE PIA DLA RFID

Na podst. opinii 9/2011 Gr. Roboczej Art. 29 nt. zmienionej propozycji sektora w sprawie ram oceny skutków w zakresie ochrony danych i prywatności w zastosowaniach RFID (WP 180) Aneks III

Privacy Risk Description and example

1. ***Unspecified and unlimited purpose***
   The purpose of data collection has not been specified and documented or more data is used than is required for the specified purpose.
2. ***Collection exceeding purpose***
   Data is collected in identifiable form that goes beyond the extent that has been specified in the purpose.
3. ***Incomplete information or lack of transparency***
   The information provided to the data subject on the purpose and use of data is not complete, data processing is not made transparent, or information is not provided in a timely manner.
4. ***Combination exceeding purpose***
   Personal data is combined to an extent that is not necessary to fulfil the specified purpose.
5. ***Missing erasure policies or mechanisms***
   Data is retained longer than necessary to fulfil the specified purpose.
6. **Invalidation of explicit consent**
   Consent has been obtained under threat of disadvantage.

OCENA SKUTKÓW W ZAKRESIE OCHRONY DANYCH OSOBOWYCH NA PRZYKŁADZIE PIA DLA RFID

Na podst. opinii 9/2011 Gr. Roboczej Art. 29 nt. zmienionej propozycji sektora w sprawie ram oceny skutków w zakresie ochrony danych i prywatności w zastosowaniach RFID (WP 180) Aneks III

Privacy Risk Description and example

7. ***Secret data collection by RFID Operator***
   Some data is secretly recorded and thus unknown to the data subject, e.g. movement profiles.
8. ***Inability to grant access***
   There is no way for the data subject to initiate a correction or erasure of his data.
9. ***Prevention of objections***
   There are no technical or operational means to allow complying with a data subject's objection.
10. ***A lack of transparency of automated individual decisions***
    Automated individual decisions based on personal aspects are used but the data subjects are not informed about the logic of the decisionmaking.
11. ***Insufficient access right management***
    Access rights are not revoked when they are no longer necessary.
12. **Insufficient authentication mechanism**
    A suspicious number of attempts to identify and authenticate are not prevented.
13. **Illegitimate data processing.** Processing of personal data is not based on consent, a contract, legal obligation, etc.

Dziękuję bardzo za uwagę

DR WOJCIECH WIEWIÓROWSKI
Wydział Prawa i Administracji Uniwersytetu Gdańskiego
Generalny Inspektor Ochrony Danych Osobowych

desiwm@giodo.gov.pl
http://edugiodo.giodo.gov.pl