Warszawa,8.03.2013

INSTRUKCJA DLA PRZEDSTAWICIELA POLSKI
na posiedzenie grupy roboczej Rady UE ds. Wymiany Informacji i Ochrony Danych (DAPIX)
13-14 marca 2013 r.

Instytucja wiodąca: Ministerstwo Administracji i Cyfryzacji
Instytucje współpracujące: Generalny Inspektor Ochrony Danych Osobowych, Ministerstwo Gospodarki, Ministerstwo Sprawiedliwości, Ministerstwo Spraw Wewnętrznych, Ministerstwo Pracy i Polityki Społecznej, Ministerstwo Zdrowia, Główny Urząd Statystyczny, Urząd Komunikacji Elektronicznej, Stałe Przedstawicielstwo RP przy UE, Ministerstwo Spraw Zagranicznych.

Informacje na temat przedstawicieli Polski na posiedzenie:	
Imię i nazwisko/stanowisko:	Aleksandra Chmielecka, główny specjalista, Departament Społeczeństwa Informacyjnego, MAC Agnieszka Wawrzyk, Radca, Wydział Sprawiedliwość i Sprawy Wewnętrzne SP RP przy UE Ewelina Zaremba, główny specjalista, Departament Analiz i Komunikacji, MAC
Delegacja towarzysząca:	Urszula Góral, Dyrektor Departamentu Edukacji Społecznej i Współpracy Międzynarodowej, Biuro Generalnego Inspektora Ochrony Danych Osobowych

PORZĄDEK OBRAD

1. **Approval of the agenda**

2. **Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)**

   - The right to be forgotten, the right data portability and profiling
   6814/13 DATAPROTECT 24 JAI 140 MI 144 DRS 37 DAPIX 35 FREMP 18 COMIX 118 CODEC 418

   - Second reading of Chapters I and II
   6828/13 DATAPROTECT 25 JAI 142 MI 147 DRS 38 DAPIX 36 FREMP 19 COMIX 119 CODEC 421

3. **Any other business**

- Certifications (poss.)
6413/13 DATAPROTECT 15 JAI 100 MI 107 DRS 24DAPIX 18 FREMP 11 COMIX 98 CODEC 332

6733/13 DATAPROTECT 21 JAI 131MI 132 DRS 35 DAPIX 31 FREMP 16 COMIX 112 CODEC 399

Stanowisko Polski do zaprezentowania podczas posiedzenia:

Stanowisko Polski do zaprezentowania:

Na wstępie Przedstawiciel Polski zaznaczy, że w stosunku do wszystkich omawianych na niniejszym posiedzeniu DAPIX przepisów zgłasza ogólne zastrzeżenie analityczne. Spowodowane jest to wciąż trwającymi konsultacjami społecznymi. Decyzje ws. ostatecznego stanowiska Polski nie zostały jeszcze podjęte.

Punkt 2 Agendy: - The right to be forgotten, the right data portability and profiling

Art. 17: Prawo do bycia zapomnianym i do usunięcia danych

Uwagi ogólne:

- Przedstawiciel zgodzi się z ogólnym kierunkiem zmian struktury artykułu 17, dzięki czemu wydaje się on obecnie bardziej przejrzysty, zaznaczając jednocześnie, że przepisy wciąż nie uzyskały wystarczającej klarowności i wymagają dalszej pracy.

- Artykuł 17 nie powinien mieć zastosowania w stosunku do zbiorów danych osobowych, prowadzonych przez organy administracji publicznej, w których dane są przechowywane i przetwarzane na podstawie przepisów prawa. Trudno jasno wysnuć taką zasadę z tego artykułu – mogłoby tu mieć zastosowanie lit. d) ust. 3, aczkolwiek wiele podmiotów publicznych w Polsce ma do tego wątpliwości, być może istnieje potrzeba wyraźniejszego tego określenia. Prośba o interpretację tego przepisu w odniesieniu do jego zastosowania przez podmioty publiczne przetwarzające dane zgodnie z prawem.

Uwagi szczegółowe:

- **- art. 17 ust. 3a (w starej wersji ust. 2)**

> ***3a.*** *Where the controller referred to in paragraph 1 has made the personal data public* ***and is obliged pursuant to paragraphs 1 and 3 to erase the data****, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data, unless this proves impossible or would involve a disproportionate effort.(...).*

Postanowienia tego przepisu w dalszym ciągu wydają się niewykonalne i niosące za sobą nadmierne i nieuzasadnione obciążenia dla administratorów.
Ten artykuł budzi w PL sporo kontrowersji zarówno wśród biznesu jak i organizacji pozarządowych.

Realizacja obowiązku poinformowania wszystkich osób trzecich, które przetwarzają upublicznione dane, o tym, że „podmiot danych wnioskuje o usuniecie wszelkich linków do danych, kopii lub replikacji" jest nie tylko trudna technicznie i kosztowna – mogłaby również prowadzić do odwrotnego efektu w postaci zwrócenia powszechnej uwagi na dane, które podmiot danych próbuje usunąć. Te zagrożenia w sposób szczególny dotyczą Internetu, gdzie obieg danych staje się coraz szybszy a wprowadzone raz dane podlegają powielaniu i rozpowszechnianiu. W tym kontekście ustalenie wszystkich osób trzecich, które przetwarzają upublicznione dane, wydaje się wręcz niemożliwe lub wymagałoby zastosowania środków stojących w sprzeczności z wolnością komunikowania się w Internecie i samą ochroną prywatności, takich jak blokowanie i filtrowanie treści.

Uzupełnienie tego przepisu o klauzulę nieproporcjonalnego wysiłku jest pewnym rozwiązaniem łagodzącym brzmienie tego artykułu aczkolwiek nie rozwiązuje wątpliwości z tym związanych. Zastosowane pojęcia są tu bardzo nieostre i pojawia się pytanie, kto miałby decydować o tym, kiedy dane działalnie może okazać się niemożliwe i będzie wymagać nieproporcjonalnego wysiłku. Takie pojęcie jest bardzo subiektywne. Administrator zawsze może uznać, że dane działalnie będzie wymagać od niego nieproporcjonalnego wysiłku, organ nadzorczy może natomiast wydać sprzeczną opinię – że taki wysiłek był uzasadniony. Może to doprowadzić do sytuacji, że administratorzy w obawie przed niekorzystną dla nich interpretacją organów nadzorczych czy wysiłek był uzasadniony czy też nie – będą na wszelki wypadek podejmować wszelkie starania prowadzące do poinformowania wszelkie podmioty trzecie o żądaniu usunięcia danych.

Większy nacisk powinniśmy kłaść na edukację i zwiększanie świadomości wśród samych użytkowników, że umieszczone przez nich raz dane w Internecie będą mogły być niemożliwe do usunięcia niż nakładać na administratorów danych nie do końca określone i kłopotliwe do spełnienia wymogi.

W związku z powyższym, **Polska jest za wykreśleniem ust. 3 a.**

Art. 17a ust. 1

> *The data subject shall have the right to obtain from the controller the restriction of the processing of personal data where:*

Należy wyjaśnić, dlaczego przyjęto dla tego artykułu sformułowanie odmienne od obecnego brzmienia art. 17 ust. 1, gdzie wyraźnie wskazane jest, że podmiot ma prawo wnioskować o usunięcie danych (*right to request* vs. *right to obtain*) oraz wzajemną relację tych dwóch przepisów. Czy ograniczenie (*restriction*) przetwarzania może lub musi być wprowadzane także z inicjatywy samego administratora danych? Czy, tak jak w oryginalnym brzmieniu art. 17 ust. 4, może to być odpowiedź na wniosek o usunięcie danych?

Art. 17a ust. 1 lit. c)

> *c) unlawful* ***processing of personal data has taken place but*** *the data subject opposes their erasure and requests the restriction of their use instead;*

Pytanie o znaczenie i cel tego przepisu? Niejasne, jak jest możliwe, aby dane które były przetwarzane niezgodnie z prawem nie podlegały usunięciu. Dlaczego podmiot danych miałby się sprzeciwiać usunięciu danych, które przetwarzane są niezgodnie z prawem? Prośba o przykłady praktyczne sytuacji, w których taki przepis miałby zastosowanie. Wydaje się też konieczne uregulowanie nowego w tym kontekście uprawnienia podmiotu, jakim byłoby „prawo do sprzeciwienia się usunięciu" (*right to object to erasure*). [czy w tej chwili administrator musi uzyskiwać zgodę na usunięcie danych albo informować o takim zamiarze?

Nowy ustęp do art. 17 a)

W celu zapewnienia spójności przepisów wnosimy o dołączenie nowego ustępu do art. 17a wyłączającego jego zastosowania do danych osobowych przetwarzanych do celów historycznych, statystycznych i naukowych, analogicznie do art. 17 ust 3 lit c.

> ***"5a. The rights provided for in paragraphs 1-4 do not apply when data are processed only for historical, statistical, or scientific purposes and the conditions in Article 83(1a) are met."***

Art. 17 b)

> *The controller shall communicate any rectification, erasure* ***or restriction of processing*** *carried out in accordance with Articles 16, 17 and 17a to each recipient to whom the data have been disclosed, unless this proves impossible or involves a disproportionate effort.*

Przedsytawiciel wspomni o potrzebie **zmiany definicji „odbiorcy" („*recipient*").** W sytuacji bardzo szerokiego zdefiniowania odbiorcy (każdy podmiot któremu ujawnia się dane) stosowanie tego przepisu może być niemożliwe do spełnienia. Należy zawęzić katalog podmiotów, które administrator obowiązany jest informować.

Brak zmiany tej definicji może prowadzić do sytuacji, kiedy administrator, który na wniosek podmiotu danych poprawiłby jego dane w swojej bazie, musiałby jednocześnie poinformować o tym fakcie wszystkich odbiorców, nawet jeśli od dawna nie łączą go z nimi żadne relacje umowne albo jeśli wprowadzone zmiany byłyby nieistotne z punktu widzenia odbiorców i podmiotu danych. W wielu przypadkach o zmianach poinformowane zostałyby podmioty, które nie przetwarzają już danych konkretnego obywatela, bo np. przekazanie danych miało charakter jednorazowy, a dane zostały już usunięte. Takie podmioty mogą być już nieuprawnione do przetwarzania danych.

W związku z tym wskazana jest zmiana definicji odbiorcy w sposób, aby wprowadzić wyłączenia lub tez należałoby zawęzić katalog odbiorców, wobec których artykuł 17b będzie stosowany.

Z kategorii odbiorców powinni zostać wyłączeni: podmioty danych oraz organy państwowe, które mogą otrzymywać dane w ramach konkretnego postępowania.

Art. 18 - Prawo przenoszenia danych

Polska nadal podtrzymuje zastrzeżenia związane z kwestiami ochrony własności intelektualnej oraz prawa konkurencji. Celem tego artykułu jest ułatwienie przenoszalności samych danych, wszelka „wartość dodatnia" uzyskana dzięki operacjom na danych wykonywanych przez administratora danych, powinna pozostać przy tym administratorze.

Dodanie **ust. 2 a** nie wydaje nam się właściwym rozwiązaniem, ze względu na **niedookreślony charakter pojęcia „prawa własności intelektualnej",** który może wywoływać spory na tle czy dana forma danych może naruszać czyjeś prawa własności intelektualnej. Z tego względu właściwszym wydaje się uzupełnienie tego artykułu, że chodzi o dane w formacie nieprzetworzonym. Z tego względu Polska zaproponuje uzupełnienie ust. 1 i 2 po słowie „data" określeniem „***in non-aggregated and/or non-modified form***", co jest lepszym rozwiązaniem niż proponowany ustęp 2a. Należy jednocześnie rozważyć, czy w każdym przypadku będzie to możliwe i ewentualnie dopuścić przekazanie danych w stanie, w jakim się aktualnie znajdują, jeżeli będzie to wygodniejsze dla administratora – nie byłoby celowe ustanawianie obowiązku doprowadzania danych do stanu wyjściowego w każdym przypadku.

Art. 20 – Środki oparte na profilowaniu

Ogólne zastrzeżenie analityczne.

> ***Ust. 1:*** *Every data subject shall have the right not to be subject to profiling which produces legal effects (...) or significant adverse effects concerning him or her* ***unless such*** *processing*

PL ma wątpliwości odnośnie wprowadzenia słowa „***adverse***" przed „*effects*". Określenie, czy efekty są negatywne czy pozytywne jest subiektywne. To, co administratorowi może się wydawać pozytywnym bądź neutralnym wpływem przez niektóre podmioty danych może zostać odebrane jako wpływ negatywny.

> ***(aa) is carried out for direct marketing purposes in relation to the exercise of freedom of expression, where the data are rendered pseudonumous and the data subject has not objected to such processing in accordance with Article 19(2); or***

Przepis w obecnym brzmieniu jest całkowicie niezrozumiały. Prosimy o wyjaśnienie związku marketingu bezpośredniego z wolnością wypowiedzi. Możliwe jest, że intencją PREZ było wymienienie 3 osobnych przypadków: marketingu, wolności wypowiedzi i danych pseudonimizowanych. Jeżeli tak jest w istocie to przepis jest sformułowany nieprawidłowo.

*(b) is (...)authorized by a Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's legitimate interests; **such processing may include processing** for fraud monitoring and prevention purposes and to ensure the security and reliability of a service provided by the controller; or*

Sformułowanie "may include" wydaje się oznaczać otwarty katalog, a nie zamknięta listę. Czy nie byłoby wskazane określenie wyczerpującego katalogu możliwych wyjątków?

Ust. 3

3. Measures based on profiling referred to in paragraph 1 shall not be based solely on the special categories of personal data referred to in Article 9

Słowo "***solely***" w tym kontekście budzi poważne zastrzeżenia i obawy. Może to bowiem oznaczać, że nie można profilować na podstawie wyłącznie danych wrażliwych. Prowadzi to w związku z tym do obawy, że jeśli profilowanie nie będzie się opierać wyłącznie na danych wrażliwych, ale również na innych danych (jak np. miejsce zamieszkania), takie profilowanie będzie dozwolone. W opinii Polski profilowanie opierające się na przetwarzaniu jakichkolwiek danych wrażliwych powinno być zabronione. Stąd wniosek o wykreślenie słowa „solely".

Ust. 4

Poparcie dla zmienionego zapisu **ust. 4:**

***4. (...)** The information to be provided by the controller under Articles 14 and 14a shall include information as to the existence of profiling **referred to in paragraph 1** and **[information concerning** the logic involved in any automatic data processing], **as well as the significance and** the envisaged consequences of such processing on the data subject.*

Punkt 2 Agendy: Second reading of Chapters I and II

Art. 2 – Zakres materialny

Article 2

Material scope

1. *This Regulation applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.*
2. *This Regulation does not apply to the processing of personal data:*
   - *(a) in the course of an activity which falls outside the scope of Union law (...);*
   - *(b) by the Union institutions, bodies, offices and agencies;*
   - *(c) by the Member States when carrying out activities which fall within the scope of Chapter 2 of the Treaty on European Union;*
   - *(d) by a natural person (...)in the course of (...) a personal or household activity;*
   - *(e) by competent **public** authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties **or other body designated under the law of the Member State concerned or Union law for those purposes.***

Ust 2 b)
Wniosek o wykreślenie tego przepisu. Biorąc pod uwagę cel reformy ODO, jakim jest harmonizacja, Rozporządzenie powinno obejmować również instytucje unijne, PL nie widzi uzasadnienia dla ich wyłączenia.

Ust 2 d)
Polska poprze zmienione brzmienie tego przepisu.

uzasadnienie:
PL nie popierała pierwotnego brzmienia artykułu, zgodnie z którym wyjątek domowy odnosił się do osób przetwarzających dane w ramach własnych działań o charakterze czysto osobistym lub domowym „w celach innych niż zarobkowe". Termin „w celach innych niż zarobkowe" powodował wątpliwości interpretacyjne i zbytnio zawężał zakres tego wyjątku. Obecne brzmienie tego przepisu nie zawiera już sformułowania „w celach innych niż zarobkowe", w związku z czym jest do zaakceptowania.

Art. 4 – Definicje

- **Odbiorca**

> *(7) 'recipient' means a natural or legal person, public authority, agency or any other body to which the personal data are disclosed whether a third party or not ; however, authorities which may receive data in the framework of a particular **inquiry** shall not be regarded as recipients*

Polska popiera zawężenie definicji **„odbiorcy" (*„recipient"*)** poprzez wyłączenie z kategorii odbiorców podmiotów publicznych, które mogą otrzymywać dane w ramach konkretnego dochodzenia. Wydaje się, że z definicji odbiorców danych powinien być również wyłączony sam podmiot danych.

Polska poprosi o doprecyzowanie i potwierdzenie, czy słowo *„**inquiry**"* należy w tym kontekście rozumieć jako zapytanie i zasieganie informacji w ramach prowadzego postępowania.
W ramach przeprowadzonych konsultacji wskazywano, ze słowo *„inquiry"* występuje w prawie unijnym i prawie polskim w kontekście spraw karnych i nie znajduje zastosowania w odniesieniu do spraw np. cywilnych, administracyjnych. Wydaje się, iż celem tego przepisu powinno być rozszerzenie wyłączenia z zakresu pojęciowego słowa „odbiorca" na organy władzy publicznej, przed którymi toczą się postępowania we wszelkich sprawach (cywilnych, karnych, administracyjnych).
Poprosimy o doprecyzowanie tego pojęcia i ew. zastąpienie go innym np. *„proceedings"*.

Uzasadnienie:
Potrzeba zmiany tej definicji wiąże się m.in. z art. 13, na podstawie którego administrator zobowiązany jest do informowania każdego odbiorcę o wszystkich operacjach poprawienia lub usunięcia danych. Brak zmiany tej definicji może prowadzić do rezultatów sprzecznych z założeniami tej reformy. Administrator, który na wniosek podmiotu danych poprawiłby jego dane w swojej bazie, musiałby jednocześnie poinformować o tym fakcie wszystkich odbiorców, nawet jeśli od dawna nie łączą go z nimi żadne relacje umowne albo jeśli wprowadzone zmiany byłyby nieistotne z punktu widzenia odbiorców i podmiotu danych. W wielu przypadkach o zmianach poinformowane zostałyby podmioty, które nie przetwarzają już danych konkretnego obywatela, bo np. przekazanie danych miało charakter jednorazowy, a dane zostały już usunięte. Takie podmioty mogą być już nieuprawnione do przetwarzania danych.

- **Dane dotyczące zdrowia**

> *(12) 'data concerning health' means such information related to the physical or mental health of an individual, which reveal information about significant health problems, treatments and sensitive conditions of an individual;*

PL wskaże na potrzebę doprecyzowania definicji danych zdrowotnych określonych w art. 4 pkt 12 poprzez uszczegółowienie i wyjaśnienie pojęcia „***sensitive conditions***". (uwaga Biura Pełnomocnika Rządu do Spraw Osób Niepełnosprawnych)

Art. 6 – Zgodność z prawem przetwarzania

PL zasugeruje uzupełnienie ust. 1 lit c) po słowach „*for compliance with a legal obligation*" o słowo „***and for exercise of a right***" (i dla wykoania uprawnienia).

> *c) processing is necessary for compliance with a legal obligation to which the controller is subject;*

Uzasadnienie: jest to brzmienie zgodne z polska ustawą o ochronie danych osobowych. Rozporządzenie powinno wprost zezwalać administratorowi na przetwarzanie danych jeśli jest to konieczne do realizacji przyznanych mu przez przepisy praw.

Art. 7 – Warunki udzielania zgody

Article 7

Conditions for consent

1. ***Where Article 6(1)(a) applies*** *the controller* ***shall be able to demonstrate*** *that consent was provided* ***by the data subject*** *.*

Polska zwróci się z prośbą o uzasadnienie ograniczenia zastosowania tego przepisu jedynie do zgody wyrażonej na podstawie art. 6.1 a). Warto zwrócić uwagę, że zgoda występuje również w art. 9 i w art. 44 i proponowane uszczegółowienie przepisu art. 7 ust. 1 może wprowadzać w błąd

Art. 8 – Przetwarzane danych osobowych dziecka

Article 8

Processing of personal data of a child

*1. For the purposes of this Regulation, in relation to the offering of information society services directly to a child, the processing of personal data of a child below the age of 13 years shall only be lawful if and to the extent that consent as referred to in Article 7 is given or authorised by the child's parent or **guardian.** The controller shall make reasonable efforts to obtain (...)consent, taking into consideration available technology.*

Stanowisko do ewentualnego wygłoszenia:

W razie podnisienia podobnej kwestii przez inne delegacje, Polska poinformuje, że nadal podtrzymuje wątpliwości związane z tym, w jaki sposób w środowisku cyfrowym administrator danych ma identyfikować, że odbiorcą jego usług jest osoba poniżej 13 roku życia, jak i w jaki sposób będzie uzyskiwało zgodę rodzica lub opiekuna. Jak w przypadku usług oferowanych na odległość dostawca usług może zweryfikować czy dana osoba jest rzeczywistym rodzicem lub opiekunem? Wiążą się z tym obawy dotyczące ochrony prywatności dzieci i opiekunów w środowisku online i zagrożeń dla ochrony prywatności Internautów

Punkt 3 Agendy: AOB - Certifications

Stanowisko Polski do zaprezentowania:

Wiarygodność mechanizmów certyfikacji w zakresie danych osobowych, pieczęci i oznaczeń w dużym stopniu zależy od kryteriów i wymogów określonych w celu ich ustanowienia, istotne jest, aby zapewnić dalsze wytyczne.
Wydaje się, że harmonizacja przepisów prawa materialnego powoduje, że do stosowania mechanizmów certyfikacji należy zachęcać w szczególności na szczeblu europejskim, a co za tym idzie określenia dalszych kryteriów i wymogów również należy dokonać na szczeblu europejskim.
Ponieważ szczegółowe określenie wszystkich kryteriów i wymogów w całości w treści rozporządzenia byłoby trudne, właściwe byłoby przyjęcie bardziej elastycznego instrumentu w celu zapewnienia dalszych kryteriów i wytycznych dotyczących mechanizmów certyfikacji w zakresie danych osobowych, w tym warunków przyznawania i odwoływania oraz wymogów w zakresie uznawania na terytorium Unii i w państwach trzecich.

Wydaje się, że najwłaściwszym instrumentem do zapewnienia pewności prawa wobec podmiotów danych, które polegają na mechanizmach certyfikacji, pieczęciach i oznaczeniach, byłby istotnie akt delegowany. (komentarz autora: popieraliśmy delegacje z art. 39.2 w tabeli opracowywanej w czasie PREZ CY).

Co do propozycji ES w zakresie korzyści związanych – PL zgłosi zastrzeżenie analityczne.

Sporządziła: Aleksandra Chmielecka, DSI MAiC (przy wykorzystaniu wkładów instytucji współpracujących)

Akceptował: Maciej Groń, Dyrektor Departamentu Społeczeństwa Informacyjnego, MAiC

DYREKTOR
DEPARTAMENTU SPOŁECZEŃSTWA INFORMACYJNEGO
MINISTERSTWA ADMINISTRACJI I CYFRYZACJI
Maciej GROŃ

Data: 8 marca 2013 r.