Warszawa, 28.04.2013

INSTRUKCJA DLA PRZEDSTAWICIELA POLSKI

na posiedzenie grupy roboczej Rady UE ds. Wymiany Informacji i Ochrony Danych (DAPIX)

29- 30 kwietnia 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:	Michał Czerniawski, Główny Specjalista, Departament Społeczeństwa Informacyjnego, MAiC Agnieszka Wawrzyk, Radca, Wydział Sprawiedliwość i Sprawy Wewnętrzne, SP RP przy UE

PORZĄDEK OBRAD

1. **Approval of the agenda**

2. **General Data Protection Regulation**

   - Second reading of Chapters I to IV

   8004/13 DATAPROTECT 35 JAI 246 MI 246 DRS 59 DAPIX 65 FREMP 35 COMIX 217 CODEC 688

3. **Any other business**

Stanowisko Polski do zaprezentowania podczas posiedzenia:

Article 22
Responsibility of the controller

Uwaga ogólna: według PL pojęcie "rights and freedoms" jest zbyt szerokie, może dotyczyć sfer całkowicie niezwiązanych z danymi osobowymi, być może należy je zawęzić (np. do „privacy"), jest to uwaga także do innych odniesień do „rights and freedoms" w projekcie rozporządzenia.

PL opowie się za przywróceniem ustępu 2, jako pomocnego do wyjaśnienia co znaczą „appropriate measures". Zaproponowana przez PL zmiana nie zmierza do poszerzenia zakresu obowiązków administratora danych, ponieważ odwołuje się do wymogów i procedur, które zostały przewidziane w innych przepisach projektowanego rozporządzenia.

PL poprze wprowadzenie w art. 22 ustępu 2a, jako przykładu zastosowania zasady rozliczalności („accountability"). Realizacja „risk-based approach" powinna być urzeczywistniona poprzez zastosowanie zasady rozliczalności, zaś zmniejszenie obowiązków administratora powinno być uzależnione od stopnia wprowadzonych działań, które umożliwiają realizację tej zasady.

Odnośnie art. 22 ust. 2a, PL poprosi o doprecyzowanie czy „restriction of personal data" należy rozumieć zgodnie z art.4 ust. 3a, czyli tylko jako przechowywanie?

Article 23
Data protection by design and by default

PL poprze wprowadzenie w art. 23 ustępu 2a. W ocenie PL rozwiązanie to może zachęcić administratorów danych do certyfikacji i wzmocnić zasadę rozliczalności.

Sugerujemy zamianę pojęcia „state of the art" na „aktualny poziom wiedzy technicznej". Wymóg stosowania najnowszych osiągnięć technicznych, wiązałby się z nadmiernymi kosztami dla administratorów danych. W ocenie PL środki odpowiadające aktualnemu poziomowi wiedzy wydają się dostatecznie dobrze chronić interesy podmiotu danych.

PL zada pytanie jaka jest intencja umieszczenia w art. 23 ust. 2 „without human intervention". W naszej ocenie ustęp ten powinien zostać doprecyzowany, tak aby dotyczył podmiotu danych. W związku z tym jesteśmy za doprecyzowaniem tego zwrotu na „without data subject intervention".

Article 24
Joint controllers

Odnośnie art. 24 ust. 2, PL zaproponuje dodanie na końcu art. 24 ust. 2 zdania umożliwiającego umówienie się pomiędzy współadministratorami co do współadministratora odpowiedzialnego i poinformowanie o tym podmiotu danych: „unless the data subject has been informed which of the joint controllers is responsible according to art. 16, 17 and 19 of this Regulation".

Article 25
Representatives of controllers not established in the Union

PL zgłosi wątpliwości odnośnie art. 25 ust. 2 lit. b, zasugeruje rozważenie czy kryterium 250 osób nie powinno zostać zastąpione kryterium liczby przetwarzanych rekordów. W naszej ocenie takie rozwiązanie odda ideę proporcjonalności i będzie się wpisywać w zasadę „risk based approach".

Do art. 25 ust. 2 lit. b odnosi się także wcześniejsza uwaga PL, czy nie należy zamiast „rights and freedoms" użyć pojęcia „privacy".

PL zgłosi także propozycję, aby pojęcie „high risks" doprecyzować jako „high risks as specified in art. 33 point 2 of this Regulation". Tak, aby to pojęcie nie budziło wątpliwości wśród administratorów danych.

PL zaznaczy, iż w różnych artykułach rozporządzenia po kryterium 250 osób występują różnie sformułowane kryteria, o podobnym znaczeniu, wskaże przy tym np. na art. 28 ust. 4 lit. b, PL proponuje, aby rozważyć czy nie należy ich ujednolicić.

Article 26
Processor

Odnośnie art. 26 ust. 2, PL opowie się przeciwko zwolnieniu z obowiązku zawierania umów o powierzenie przetwarzania podmiotów z tej samej grupy kapitałowej, czyli poprze usunięcie zaznaczonego nawiasami fragmentu. W ocenie PL zawieranie takich umów nie będzie dla przedsiębiorców utrudnieniem, w Polsce przedsiębiorcy należący do jednej grupy już je zawierają, jest to standardowa umowa, a wpłynie na poprawę ochrony danych.

Odnośnie art. 26 ust. 3, PL zwróci uwagę, iż zgodnie z polskim prawem formą ekwiwalentną do formy pisemnej jest forma elektroniczna z kwalifikowanym podpisem elektronicznym, która wciąż nie jest powszechna wśród przedsiębiorców. W związku z tym jesteśmy za tym, aby wyraźnie dopuścić do formy pisemnej, jako równoważną, formę elektroniczną.

PL opowie się za usunięciem art. 26 ust. 4a, jako nakładającego obowiązek, którego wielu, zwłaszcza małych, procesorów, nie będzie w stanie realizować. Zwracamy uwagę, iż umowa pomiędzy administratorem danych a procesorem może przewidywać kary za jej niewykonanie, tak więc procesorzy będą mieli do wyboru albo niewykonanie obowiązku z ust. 4a albo karę umowną.

Article 28
Records of categories of processing activities

Odnośnie art. 28 ust. 1, PL podtrzyma uwagę z przypisu 385, aby doprecyzować, że dokumenty/rekordy mogą być przechowywane w formie papierowej lub elektronicznej.

PL w art. 28 ust. 1 lit. c opowie się za przywróceniem „legitimate interest" tak jak było w wersji wyjściowej. Słuszny interes administratora jest specyficzną podstawą przetwarzania danych, na którą powinniśmy zwracać szczególną uwagę. Stąd administrator powinien wskazywać sytuacje, w których powołuje się na tą przesłankę.

Odnośnie art. 28 ust. 1 lit. e, PL zwróci się do PREZ o doprecyzowanie, co znaczy „regular", można to sformułowanie dopracować np. w motywie.

W art. 28 ust. 2a, PL zaproponuje dodania, jako obowiązkowego, rekordu dotyczącego „the (...) regular categories of recipients of the personal data". Chodzi nam o to, aby procesor był zobowiązany prowadzić listę subprocesorów, taka informacja jest niezwykle istotna z punktu widzenia zapewnienia kontroli nad danymi osobowymi.

W art. 28 ust. 2a lit. d, PL wniesie o dodanie na końcu zdania "provided that the proccessor is transferring such data", taka by doprecyzować, że chodzi o dane, które transferuje procesor.

Odnośnie art. 28 ust. 4, PL powtórzy wcześniejszą uwagę z art. 25 ust. 2 lit. b, dotyczącą tego, że kryterium to powinno zostać oparte na ilości rekordów a nie liczbie pracowników.

PL powtórzy także uwagę dotyczącą możliwości ujednolicenia kryteriów występujących wraz kryterium liczby pracowników (por. uwaga z art. 25 ust. 2 lit. b.

PL opowie się także za doprecyzowaniem, iż kryteria z art. 28 ust. 4 lit. b i c są stosowane rozłącznie, tj. wystarczy, że zaistnieje jedno z nich.

Article 31
Notification of a personal data breach to the supervisory authority

PL wniesie o usunięcie z motywu 70 pojęcia „moral damage" – w polskim systemie prawnym każde naruszenie prywatności jest naruszeniem dóbr osobistych i umożliwia wytoczenie powództwa cywilnoprawnego. W związku z tym każde naruszenie prywatności wywołuje „moral damage".
W zakresie art. 31 ust. 1, PL zajmie stanowisko, iż każde naruszenie danych osobowych niesie ze sobą negatywny skutek dla podmiotu danych. W ocenie PL zamiast „adversely" powinno zostać użyte pojęcie „significantly", tak, aby ograniczyć zakres zgłaszanych naruszeń tylko do tych, które rzeczywiście wpływają na sytuację podmiotu danych natomiast pojęcie praw i wolności (rights and freedoms) podmiotu danych, tak jak to PL zgłaszało do wcześniejszych artykułów, powinno zostać zastąpione pojęciem „privacy" (prywatność). Obecne sformułowanie jest niezwykle szerokie, przez co może skutkować zalewem nieistotnych zgłoszeń.
Odnośnie art. 31 ust. 1a, PL zajmie stanowisko, iż pomimo podjęcia działań przewidzianych w art. 32 ust. 3 lit. b, administrator powinien powiadomić organ nadzoru o naruszeniu, tak aby mógł on ocenić czy administrator podjął właściwe działanie. W związku z tym PL wypowie się przeciwko dodaniu ust. 1a w zaproponowanym brzmieniu.

PL opowie się za usunięciem art. 31 pkt 5 i 6, przewidujących delegację dla Komisji Europejskiej, uznając, iż taka delegacja wprowadza element niepewności dla administratora danych.

Article 32
Communication of a personal data breach to the data subject

PL podtrzyma zastrzeżenie z przypisu 439, aby doprecyzować, iż forma pisemna i elektroniczna są równoważne.

W zakresie art. 32, PL zgłosi analogiczne uwagi, jak do art. 31. PL zajmie stanowisko, iż każde naruszenie danych osobowych niesie ze sobą negatywny skutek dla podmiotu danych. W naszej ocenie zamiast „adversely" powinno zostać użyte pojęcie „significantly", tak, aby ograniczyć zakres zgłaszanych naruszeń tylko do tych, które rzeczywiście wpływają na sytuację podmiotu danych natomiast pojęcie praw i wolności (rights and freedoms) podmiotu danych powinno zostać zastąpione pojęciem „privacy" (prywatność).Obecne sformułowanie jest niezwykle szerokie, przez co może skutkować zalewem nieistotnych zgłoszeń.

PL opowie się za usunięciem art. 32 ust. 5 i 6, przewidujących delegację dla Komisji Europejskiej, uznając iż taka delegacja wprowadza element niepewności dla administratora danych.

Article 33
Data protection impact assessment

PL zaznaczy, że w art. 33 powinno być wyraźne odniesienie do art. 23 (privacy by design i by default), tak aby podkreślić związek między tymi dwoma rozwiązaniami, w szczególności, okoliczność, iż PIA powinno obejmować także analizę w zakresie privacy by design i privacy by default.

Odnośnie art. 33 ust. 1 lit. e oraz ust. 2a oraz 2b, PL zajmie stanowisko, iż lepiej by kompetencja ta zamiast krajowym organom nadzoru, była przyznana Europejskiej Radzie Ochrony Danych. Przyznanie jej krajowym organom nadzoru kreuje element dużej niepewności dla administratorów danych.

Article 34
Prior (...) consultation

Odnośnie art. 34 ust. 2, PL opowie się za wykreśleniem przetwarzającego jako zobowiązanego do konsultowania się z organem ochrony danych. To administrator danych zakreśla cel i zakres przetwarzania danych, a co za tym idzie – tylko on powinien być zobowiązany do dokonywania takich ustaleń. W ocenie PL dla wielu procesorów, szczególnie małych, takie rozwiązanie mogłoby być zbyt uciążliwe.

PL zgłosi uwagę ogólną – zapyta o zastosowanie tego przepisu do sektora publicznego czy np. zakaz przetwarzania na podstawie art. 34 ust. 3 i 3a nie spowoduje paraliżu funkcjonowania organów publicznych

PL poprosi PREZ o doprecyzowanie jak obowiązek z art. 34 ust. 7 ma się do obowiązku z art. 52 ust. 1 lit. f ? Czy nie jest to powtórzenie tamtego obowiązku?

PL opowie się za wykreśleniem delegacji dla KE z art. 34 ust. 8 jako zbędnej.

Article 35
Designation of the data protection officer

Odnośnie art. 35 ust. 1, PL poprze zaproponowaną zmianę, która uwzględnia nasze wcześniejsze uwagi. Powszechny obowiązek wyznaczenia inspektora ochrony danych osobowych byłby niezwykle uciążliwy zwłaszcza dla małych i średnich przedsiębiorców.

Polska opowie się za dodaniem ustępu sankcjonującego powoływanie zastępców inspektora ochrony danych. W niektórych, zwłaszcza większych podmiotach, pojedynczy inspektor może nie wystarczyć, inspektor nie będzie też obecny w przedsiębiorstwie cały czas. Proponujemy w związku z tym dodanie w art. 35 ustępu 1a stanowiącego, iż „the controller or the processor may appoint one or more deputy data protection officers. Deputy data protection officer must fulfill conditions stipulated in art. 35 point 5 of this Regulation".

W art. 35 ust. 5 sugerujemy wprowadzenie wymogu, aby inspektorem ochrony danych nie mogła być osoba prawomocnie skazana za przestępstwo z winy umyślnej. Inspektor ochrony danych musi mieć nieposzlakowaną opinię i gwarantować prawidłowe wykonywanie swojej funkcji. W związku z tym sugerujemy dodanie na końcu art. 35 ust. 5 zdania: „A person designated as a data protection officer cannot have a criminal record resulting from a criminal offence due to intentional guilt".

Odnośnie art. 35 ust. 7, w związku z usunięciem z rozporządzenia postanowień dotyczących kadencji inspektora, sugerujemy usunięcie w tym ustępie "during their term of office" jako zbędnego.

Odnośnie art. 35 ust. 10 to postanowienie jest niezwykle szerokie, być może wymaga doprecyzowania, Polska poprosi w szczególności o wyjaśnienie czy kontakt ze strony podmiotu danych kreuje po stronie administratora danych jakieś konkretne obowiązki, niezależne od wagi zapytania?

Article 37

Tasks of the data protection officer

Odnośnie art. 37 Polska poprosi o doprecyzowanie czy obecne brzmienie art. 37 ust. 1 lit. b obejmuje także monitorowanie rekordów, o których mowa w art. 28 rozporządzenia. A także czy obejmuje monitorowanie notyfikacji naruszeń danych osobowych, o których mowa w art. 31 i 32 rozporządzenia.

Sporządził: Michał Czerniawski, DSI MAiC (przy wykorzystaniu wkładów instytucji współpracujących)

Akceptował: Maciej Groń, Dyrektor Departamentu Społeczeństwa Informacyjnego, MAiC

DYREKTOR
DEPARTAMENTU SPOŁECZEŃSTWA INFORMACYJNEGO
MINISTERSTWA ADMINISTRACJI I CYFRYZACJI

Data: 28 kwietnia 2013 r.

Maciej GROŃ
