Warszawa, 24.01.2013

INSTRUKCJA DLA PRZEDSTAWICIELA POLSKI
na posiedzenie grupy roboczej Rady UE ds. Wymiany Informacji i Ochrony Danych (DAPIX)
29 -30 stycznia 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, Urząd Ochrony Konkurencji i Konsumentów, Ministerstwo Finansów, Ministerstwo Kultury i Dziedzictwa Narodowego, Stałe Przedstawicielstwo RP przy UE, Ministerstwo Spraw Zagranicznych.

Informacje na temat przedstawicieli Polski na posiedzenie:	
Imię i nazwisko/stanowisko:	Jarosław Łuba, radca ministra, Departament Społeczeństwa Informacyjnego, Ministerstwo Administracji i Cyfryzacji Agnieszka Wawrzyk, Radca, Wydział Sprawiedliwość i Sprawy Wewnętrzne SP RP przy UE
Delegacja towarzysząca:	

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)**

   Article-by-article discussion: Chapters VIII, IX, X and XI
   16529/12 DATAPROTECT 133 JAI 820 MI 754 DRS 132 DAPIX 146 FREMP 142 COMIX 655 CODEC 2745

Stanowisko Polski do zaprezentowania podczas posiedzenia:

Rozdział VIII – Środki ochrony prawnej, odpowiedzialność i sankcje (art. 73-79)

Artykuł 73 - Prawo do złożenia skargi do organu nadzorczego
Dotyczy: Artykuł 73 przewiduje prawo każdego podmiotu danych do złożenia skargi do organu nadzorczego w dowolnym państwie członkowskim, podobnie jak na podstawie art. 28 ust. 4 dyrektywy 95/46/WE. Wymienia on ponadto organy, organizacje lub zrzeszenia, które mogą składać skargi w imieniu podmiotu danych lub, w przypadku naruszenia ochrony danych osobowych, niezależnie od skargi podmiotu danych.

Uwagi:
Proponuje się albo usunięcie ust. 2 i 3 albo doprecyzowanie mandatu w jakim mogłyby działać organizacje. lub zrzeszenia, które mogą składać skargi w imieniu podmiotu danych. Można również rozważyć wprowadzenie przepisu, który zagwarantowałby, że właściwy jest art. 51 np. „Takie uprawnienie pozostaje bez uszczerbku dla postanowień art. 51 określającego właściwość organu nadzorczego."

Uzasadnienie:
W ocenie przedsiębiorców i sektora finansowego nie ma żadnego powodu, aby tak szeroko i nieprecyzyjnie zdefiniowany katalog podmiotów miał prawo składania skarg bez wykazania interesu prawnego. Jego przyjęcie pozwoliłoby dowolnym organizacjom, które przyjmą miano „organizacji chroniącej prawa podmiotów danych" na składanie skarg do organów nadzorczych w imieniu jednego lub większej liczby podmiotów jeżeli arbitralnie uznają, że prawa podmiotu zostały naruszone. Stawiałoby to administratora danych w całkowitej nierównowadze w stosunku do tych organizacji. Przepis ten powoduje trudne do przewidzenia skutki: tworzenia organizacji „broniących interesów podmiotów danych", których wiarygodność i legalność działania trudno zweryfikować, oraz lawinę pozostających poza kontrolą podmiotu danych skarg, i mnogość postępowań, i.t.p. Konieczne jest doprecyzowanie, że prawo podmiotu danych do złożenia skargi w dowolnym państwie nie podważa, kluczowej dla funkcjonowania firm, zasady „jednego okienka', wprowadzonej w art. 51.
W ocenie organizacji konsumenckiej BEUC (Bureau europeen des unions de consommateurs), zrzeszającej organizacje konsumenckie z UE, projektowane przepisy dające prawo do złożenia skargi są korzystne z punktu widzenia podmiotu danych, który dotychczas miał większą trudność dochodzenia praw. Jednak nowe przepisy nie wskazują precyzyjnie, kto będzie ponosił koszty tłumaczeń i podróży skarżących. Organizacja, inaczej niż przedsiębiorcy i sektor finansowy przychylnie odnoszą się nowych praw dla podmiotów, organizacji i zrzeszeń działających w imieniu podmiotów danych. Według opinii Europejskiego Inspektora Ochrony Danych (EDPS) z 7 marca 2012 r. powinien być natomiast doprecyzowany mandat działania organizacji działających w imieniu podmiotów danych (ust. 2 i 3), a także zapewnione odpowiednie mechanizmy składania pozwów zbiorowych.

Artykuł 74 - Prawo do sądowego środka ochrony prawnej przeciwko organowi nadzorczemu
Dotyczy: Artykuł 74 dotyczy prawa do skorzystania z sądowego środka ochrony prawnej przeciwko organowi nadzorczemu. Opiera się on na przepisie ogólnym art. 28 ust. 3 dyrektywy 95/46/WE. Artykuł ten ustanawia w szczególności sądowy środek ochrony prawnej zobowiązujący organ nadzorczy do podjęcia działania w odpowiedzi na skargę oraz wyjaśnia kompetencje sądów państwa członkowskiego, w którym organ nadzorczy ma siedzibę. Przewiduje ponadto możliwość wszczęcia przez organ nadzorczy państwa członkowskiego, w którym podmiot danych ma miejsce zamieszkania, postępowania sądowego w imieniu podmiotu danych przed sądami innego państwa członkowskiego, w którym ma siedzibę właściwy organ nadzorczy.

Uwagi:
Ust. 5 dotyczy obowiązku wykonywania prawomocnych orzeczeń sądów. Delegacja PL poprosi o doprecyzowanie co ma oznaczać ten przepis. Jeśli ma z niego wynikać obowiązek wykonywnaia orzeczeń sądów innych państw członkowskich, to delegacja zwrócić uwagę, iż np. w PL środek ochrony prawnej przewidziany w art. 74 projektu byłby rozpatrywany przez sądy administracyjne.
Nie wyjaśniono ponadto w projekcie pojęcia „sądowy środek ochrony prawnej", tzn. czy w ramach tej instytucji podmiotom danych przysługuje także prawo do odszkodowania.

Uzasadnienie:

Dotychczasowe brzmienie oznaczałoby, że w PL należałoby fundamentalnie zmienić system ochrony prawnej na ten o charakterze cywilnym lub karnym, gdyż obowiązujące prawo unijne nie reguluje kwestii wykonywania orzeczeń sądów administracyjnych. W ocenie Polski przepis byłby bardzo problematyczny do stosowania.

Artykul 75 - Prawo do sądowego środka ochrony prawnej przeciwko administratorowi lub podmiotowi przetwarzającemu

Dotyczy: Artykuł 75 dotyczy prawa do sądowego środka ochrony prawnej przeciwko administratorowi lub podmiotowi przetwarzającemu, w oparciu o art. 22 dyrektywy 95/46/WE, i umożliwia skierowanie sprawy do sądu bądź w państwie członkowskim, w którym ma siedzibę pozwany, bądź w tym, w którym ma miejsce zamieszkania podmiot danych. Jeśli postępowanie w ten samej sprawie czeka na rozstrzygnięcie w ramach mechanizmu zgodności, sąd może zawiesić swoje postępowanie, z wyjątkiem sytuacji nadzwyczajnych.

Uwagi:

Właściwa jest uwaga zawarta w poprzednim punkcie. Jak się wydaje art. 75 projektu dotyczy środków o charakterze cywilnym, ewentualnie karnym, co wykluczałoby problem z wykonywaniem orzeczeń sądów innych państw członkowskich wskazany ad. art. 74 projektu, gdyż kwestie te są uregulowane na poziomie unijnym. Np. kwestia wykonywania orzeczeń w sprawach cywilnych jest regulowana rozporządzeniem nr 44/2001. W przypadku ust.3 – niewątpliwie korzystnym dla właściwego stosowania rozporządzenia, byłoby sprecyzowanie użytego w tym przepisie pojęcia „pilny charakter spraw" (czy można wskazać choćby przykladowe sytuacje, w których spełniona byłaby taka przesłanka).

Uzasadnienie:

EDPS zwraca uwagę na możliwość powstania trudnych sutuacji z punktu widzenia jurysdykcji z zaangażowaniem sądu właściwego dla podmiotu danych i organu nadzorczego administratora/podmiotu przetwarzającego. Zwraca też uwagę na niedoskonałości przepisów, gdy postępowanie dotyczy sporów, kiedy pozwanym jest organ publiczny.

Artykul 76 - Wspólne zasady postępowań sądowych

Dotyczy: Artykuł 76 przedstawia wspólne zasady postępowań sądowych, w tym prawa organów, organizacji lub zrzeszeń do reprezentowania podmiotów danych przed sądami, prawo organu nadzorczego do udziału w postępowaniach prawnych oraz uzyskiwania przez sądy informacji na temat postępowań prowadzonych równolegle w innym państwie członkowskim, a także możliwość zawieszania przez sądy postępowań w takich przypadkach[1]. Na państwie członkowskim ciąży obowiązek zapewnienia sprawnego przebiegu postępowań sądowych[2].

Uwagi:

Brak uwag.

Dodatkowe informacje do wiadomości delegacji Polskiej:

Organizacja konsumencka BEUC popierając kształ przepisu, sugeruje równocześnie niekonsekwencję i brak przepisów dotyczących instytucji pozwu zbiorowego, już dość dobrze upowszechnionej w państwach członkowskich UE. GIODO nie widzi jednak możliwości wprowadzenia w Polsce pozwu zbiorowego w

---

[1] Na podstawie art. 5 ust. 1 decyzji ramowej Rady 2009/948/WSiSW z dnia 30 listopada 2009 r. w sprawie zapobiegania konfliktom jurysdykcji w postępowaniu karnym, Dz.U. L 328 z 15.12.2009, s. 42 oraz art. 13 ust. 1 rozporządzenia Rady (WE) nr 1/2003 z dnia 16 grudnia 2002 r. w sprawie wprowadzenia w życie reguł konkurencji ustanowionych w art. 81 i 82 Traktatu, Dz.U. L 1 z 4.1.2003, s. 1.

[2] Na podstawie art. 18 ust. 1 dyrektywy 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych uslug społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym), Dz.U. L 178 z 17.7.2000, s. 1.

kwestii ochrony danych osobowych. EDPS zwraca natomiast uwagę na potrzebę doprecyzowania przepisów dotyczących właściwości sądów.

Artykuł 77 - Prawo do odszkodowania i odpowiedzialność
Dotyczy: Artykuł 77 ustanawia prawo do odszkodowania i zasady odpowiedzialności. Opiera się on na art. 23 dyrektywy 95/46/WE, rozszerza to prawo na szkody spowodowane przez podmioty przetwarzające i wyjaśnia zasady odpowiedzialności współadministratorów i podmiotów współprzetwarzających. Przewiduje, iż każda osoba, która poniosła szkodę w wyniku niezgodnej z prawem operacji przetwarzania danych lub działania niezgodnego z przepisami ustanowionymi w niniejszym rozporządzeniu, ma prawo do odszkodowania od administratora lub podmiotu przetwarzającego.

Uwagi:
W przepisie tym nie wskazano jaki sąd będzie właściwy w przypadku, gdy przetwarzanie danych osobowych odbywa się w kontekście działalności administratora lub podmiotu przetwarzającego ustanowionych na terytorium Unii, a administrator lub podmiot przetwarzający prowadzą działalność w więcej niż jednym państwie członkowskim. Należy również doprecyzować koncepcje odpowiedzialności solidarnej, tak aby podmiot danych mógł przede wszystkim wystąpić z wnioskiem o odszkodowanie do administratora.

Uzasadnienie:
Organizacja konsumencka BEUC proponuje dalsze poszerzenie przepisu, aby prawo do odszkodowania od administratora lub podmiotu przetwarzającego mogła wystąpić organizacja reprezentująca poszkodowane podmioty danych. Można też sporządzić katalog przewinień i potencjalnych odszkodowań. Wspólna reprezentacja jest skuteczniejsza, bo obecny przepis mógłby być „martwy" z uwagi na indywidualną skalę naruszenia, koszty dochodzenia roszczenia podmiotu danych. Np. skuteczniejsze byłoby kolektywne dochodzenie naruszeń wycieku danych kart kredytowych. Organizacja konsumencka przychylnie odnosi się do koncepcji odpowiedzialności solidarnej.
Z drugiej strony sektor finansowy zwraca uwagę, że przyjęcie odpowiedzialności solidarnej z podmiotem, któremu powierzono dane do przetwarzania, za szkody wynikłe z niezgodnego z prawem przetwarzania danych spowoduje, że roszczenie podmiotów danych w praktyce zawsze będą kierowane do banków, które będą zmuszone, niezależnie od stopnia zawinienia, czy też nawet braku zawinienia do ponoszenia odpowiedzialności za działania podmiotu, któremu przetwarzanie danych powierzyły.
EDPS zwraca uwagę na niepraktyczność ust. 2, który zobowiązuje podmiot danych do wnioskowania o odszkodowanie łącznie administratora i podmiot przetwarzający. Trudno jest podmiotowi danych określić zakres przewinień tych podmiotów, stąd sugerowana jest zmiana przepisów na rzecz możliwości zgłoszenia wniosku o odszkodowanie do administratora.

Artykuł 78 - Kary
Dotyczy: Artykuł 78 zobowiązuje państwa członkowskie do ustanowienia przepisów dotyczących kar, nakładania kar za naruszenia rozporządzenia oraz zapewnienia wdrożenia jego przepisów.

Uwagi:
Przepis ten dotyczy kar mających zastosowanie w przypadku naruszenia przepisów o ochronie danych osobowych. Określenie tych kar jest zbyt ogólne i wymaga doprecyzowania.

Artykuł 79 - Sankcje administracyjne
Dotyczy: Artykuł 79 zobowiązuje każdy organ nadzorczy do nakładania sankcji administracyjnych wymienionych w katalogu zawartym w tym przepisie, w postaci grzywien do kwoty maksymalnej, z należytym uwzględnieniem każdego indywidualnego przypadku.

Dodatkowe informacje do wiadomości delegacji Polskiej:
Projekt rozporządzenia był przedmiotem opinii komisji JURI (Prawo) i ITRE (Przemysł, Badania Naukowe i Energia) Parlamentu Europejskiego. W zakresie tego artykułu komisja JURI proponuje wykreślenie części szczegółowych przepisów stanowiących o sankcjach i pozostawienie swobody w ich kształtowaniu organowi

nadzorczemu przy pozostawieniu górnej ich granicy (do 1 000 000 EUR lub 2% obrotu). Komisja ITRE chce znacznego ograniczenia sankcji administracyjnych poprzez uzależnienie kwoty nakładanej grzywny od tego czy dane są danymi szczególnie chronionymi, czy praktyka niezgodnego z prawem przetwarzania danych ma charakter powtarzający się. ITRE proponuje m.in. usunąć wyszczególnienie przewinień. Ponadto ITRE pragnie doprecyzowania roli organów nadzorczych w odniesieniu do sankcji. Sankcje mogą być nakładane jedynie na administratorów i podmioty przetwarzające, którzy posiadają główną siedzibę w tym samym państwie członkowskim. W uwagach zdefiniowano wzajemne obowiązki organów nadzorczych wobec siebie w ramach mechanizmu spójności, doprecyzowano również obowiązki informacyjne o środkach odwoławczych od decyzji organów nadzorczych.
Przedłożona została również opinia Pana Jana Albrechta, posła sprawozdawcy dla opiniowanego rozporządzenia w komisji LIBE (Wolności Obywatelskie, Sprawiedliwość i Sprawy Wewnętrzne). Opinia jest analizowana, niemniej niektóre uwagi mogą być wykorzystane do argumentacji uwag na poziomie grupy roboczej – opinia stanowi załącznik do instrukcji.
Punkt dotyczący sankcji administracyjnych był przedmiotem dyskusji ministrów na nieformalnym posiedzeniu Rady (Sprawiedliwości i Spraw Wewnętrznych) w Dublinie w dn. 17-18 stycznia br. Ministrowie wyrazili szerokie poparcie nadaniu krajowym organom nadzorczym większej elastyczności w zakresie wysokości kar oraz innych alternatywnych środków takich jak ostrzeżenia, upomnienia i inne łagodniejsze środki z zakresu nadzoru.

Uwaga ogólna:
W opinii interesariuszy z sektora przedsiębiorców i finansowego wynika, że sankcje przewidziane projektem są znaczne i nieadekwatne do zakresu naruszeń. Sankcje wydają się zbyt restrykcyjne i zbyt wysokie, bardzo ważne jest podkreślenie proporcjonalnego charakteru sankcji, również z punktu widzenia rentowności i sytuacji przedsiębiorstw w różnych krajach i różnych sektorach. Ważne jest aby każdy przypadek nałożenia sankcji rozpatrywany był przez organ ochrony danych indywidualnie, istotne jest zachowanie w tym zakresie dużej dozy samodzielności i szerokiego pola manewru dla organu nadzorczego. Czynniki brane pod uwagę przy określaniu wysokości sankcji wskazane w ust. 2 wydają się właściwie wskazane, zarówno w opinii sektora przedsiębiorstw, banków i organizacji konsumenckich. Przychylnie do kwestii możliwości nakładania sankcji administracyjnych odnosi się także EDPS, z zastrzeżeniem pozostawienia większej elastyczności ich nakładania przez krajowe organy nadzorcze. Dotyczy to zwłaszcza obszarów, które mają zostać regulowane aktami delegownymi bądź wykonawczymi (np. notyfikacje naruszeń, „privacy by deisgn"). Art. 79 nie wyjaśnia również możliwości nakładania sankcji kumulatywnych (za kilka naruszeń) lub rozwiązania które będzie zapobiegało sytuacji, że kilka DPA nałoży sankcje na dane przedsiębiorstwo za to samo. Czy rozumiemy, że karę nakłada jedynie DPA, w którego kraju administrator ma „main establishment"?
Sygnalizacyjnie należy zwrócić uwagę na stosowaną w tym przepisie terminologię – „umyślnie lub lekkomyślnie", która może budzić pewne wątpliwości na gruncie polskiego języka prawnego (jak wiadomo w prawie karnym rozróżnia się winę umyślną oraz winę nieumyślną występującą w dwóch formach lekkomyślności i niedbalstwa), tj. czy rozwiązanie to obejmuje wszystkie formy winy nieumyślnej w rozumieniu polskiego prawa karnego?
Inną kwestią są wątpliwości konstytucyjne zgłaszane przez ekspertów czy polski organ nadzorczy może nakładać sankcje administracyjne, o których mowa w projekcie rozporządzenia. W Polsce sankcje administracyjne są nakładane na gruncie przepisów karnych, i nie są badane przesłanki takie jak umyślność bądź nieumyślność naruszeń, o których mowa w ust. 2 i 3 tego artykułu. W tym kontekście można zachować wyszczególnienie przewinień, za które grożą sankcje, co daje większą pewność prawną administratorom. W tym celu suegruje się wprowadzenie słowa „może" – „organ nadzorczy może nałożyć grzywnę" w poszczególnych przepisach (ust.4 i ust. 5 „The supervisory authority may impose a fine"). Gdyby panowała zgoda co takiego kierunku prac, Polska chciałaby zaproponować następujące rozwiązania szczegółowe.

Uwagi szczegółowe:
a) ad. ust. 1

W ust. 1 konieczne jest doprecyzowanie, że do nakładania sankcji przewidzianych w artykule 79 uprawniony jest nie każdy, a właściwy zgodnie z artykułem 51, organ nadzorczy. Sugeruje się zatem zamianę „Każdy organ nadorczy" na „Organ nadzorczy, właściwy zgodnie z art. 51"

b) ad. ust. 2
Wskazane jest pozostawienie organom nazdorczym większej dozy elastyczności w zakresie nie nakładania sankcji - rozszerzenie możliwości stosowania w pierwszej kolejności procedury ostrzegawczej (ostrzeżenia i upomnienia) i dopiero w przypadku powtarzających się naruszeń bądź ze względu na wysoką powagę i szkodliwość tych naruszeń – wprowadzenie możliwości karania grzywnami. Np. w stosunku do niektórych przypadków organy nazorcze powinny móc stosować ostrzeżenia, w szczególności jeżeli naruszenie nie będzie miało lub w nieznacznym stopniu wpływ na podmiot danych lub gdy nie zagrozi prawom podmiotu danych. Przykładem może być ust 4 - zastosowanie niewłaściwego formatu, jeżeli będzie on mógł być odczytany przez podmiot danych i nie spowoduje niemożliwości zaznajomienia się ze swoimi danymi, powinien móc podlegać jedynie ostrzeżeniu.

Ewentualnie gdyby była taka potrzeba, można wprowadzić następujące zmiany do ust. 2. Należy dodać po słowie „czasu trwania naruszenia" następujący tekst: „sensytywności danych naruszonych, umyślnego lub lekkomyślnego charakteru naruszenia, zakresu szkód lub zagrożenia znaczącymi szkodami stworzonego przez naruszenie, stopnia odpowiedzialności..." i dalej zgodnie z dotychczasowym brzmieniem. Należy również dodać zdanie: „Nakładając grzywnę administracyjną organa nadzorcze będą także brały pod uwagę grzywny, odszkodowania i inne kary uprzednio nałożone przez sąd lub inny organ na osobę fizyczną lub prawną w związku z danym naruszeniem".
Proponuje się również następujące przepisy precyzujące warunki nakładania kar administracyjnych z górnych zakresów w ust. 4-6:
2a. Okoliczności obciążające prowadzące do nakładania kar administracyjnych z górnych zakresów określonych w ustępach 4 do 6 będą w szczególności obejmowały:
(i) wielokrotne naruszenia popełniane z rażącym lekceważeniem obowiązującego prawa,
(ii) odmowę współpracy lub utrudnianie postępowania egzekucyjnego, oraz
(iii) naruszenia dokonywane umyślnie, poważne i rokujące spowodowanie znaczących szkód.
2b. Okoliczności łagodzące prowadzące do nakładania kar administracyjnych z dolnych zakresów będą obejmowały:
(i) podjęcie przez osobę fizyczną lub prawną działań mających zapewnić zgodność z właściwymi wymogami,
(ii) autentyczną niepewność co do tego, czy działanie stanowiło naruszenie danych obowiązków,
(iii) bezzwłoczne zaprzestanie naruszenia z chwilą uzyskania o nim wiedzy, oraz
(iv) współpracę w każdym procesie egzekucyjnym.

c) ad. ust. 3
W opinii Polski kluczowe jest wprowadzenie fazy przejściowej pomiędzy poinformowaniem administratorów i przetwarzających danych o naruszeniu a faktycznym nałożeniem sankcji. Proponuje się zatem usunięcie części ust. 3 po fragmencie „na piśmie" do końca tego ustępu.

d) ad. ust. 4
Należy podkreślić, że przypisanie poszczególnych kategorii naruszeń do poszczególnych maksymalnych poziomów kary będzie ostatecznie możliwe po uzgodnieniu zapisów konkretnych artykułów i ew. przeformułowaniu i wyjaśnieniu zapisów, które nie są jeszcze do końca jasne. Warto rozważyć wprowadzenie dla osób i podmiotów, które dopuściły się naruszenia możliwości usunięcia naruszenia bądź przyjęcia wyznaczonych przez organ nadzorczy odpowiednich środków zaradczych w celu uniknięcia sankcji.
Proponuje się wprowadzenie następujących zmian w ust. 4:
- zastąpienie sformułowania „Organ nadzorczy nakłada grzywnę do wysokości 250 000 EUR lub w przypadku przedsiębiorstwa do 0,5 % jego rocznego światowego obrotu, na każdy podmiot, który umyślnie lub lekkomyślnie:" sformułowaniem „Organ nadzorczy może nałożyć łącznie grzywnę w wysokości do 250

000 EUR, lub w przypadku przedsiębiorstwa do 0,5% jego rocznego światowego obrotu do maksymalnie 500 000 EUR za każdy przypadek , na każdy podmiot, który umyślnie naruszając prawo lub z rażącym lekceważeniem stosownych obowiązków:

e) ad. ust. 5
Podobne zmiany można wprowadzić w ustępie 5 poprzez zamianę sformułowania „Organ nadzorczy nakłada grzywnę do wysokości 500 000 EUR lub w przypadku przedsiębiorstwa do 1 % jego rocznego światowego obrotu, na każdy podmiot, który umyślnie lub lekkomyślnie:" na „Organ nadzorczy może nałożyć łącznie grzywnę w wysokości do 500 000 EUR, lub w przypadku przedsiębiorstwa do 1 % jego rocznego światowego obrotu, do maksymalnie 1 000 000 EUR za każdy przypadek , na każdy podmiot, który, umyślnie naruszając prawo lub z rażącym lekceważeniem stosownych obowiązków:"

f) ad. ust. 6
I konsekwentnie zmiany należy wprowadzić do ustępu 6 poprzez zamianę sformułowania „Organ nadzorczy nakłada grzywnę do wysokości 1 000 000 EUR lub w przypadku przedsiębiorstwa do 2 % jego rocznego światowego obrotu, na każdy podmiot, który umyślnie lub lekkomyślnie:" na „Organ nadzorczy może nałożyć łącznie grzywnę w wysokości do 1 000 000 EUR lub w przypadku przedsiębiorstwa do 2 % jego rocznego światowego obrotu, do maksymalnie 2 000 000 EUR za każdy przypadek , na każdy podmiot, który, umyślnie naruszając prawo lub z rażącym lekceważeniem stosownych obowiązków:"

g) ad. ust. 7
Proponuje się usunięcie delegacji do wydania aktu delegowanego dla Komisji Europejskiej w celu aktualizacji kwot grzywien określonych w ustępach 4-6.

Uzasadnienie:
a) ad. ust. 1
Dotychczasowy zapis ust. 1 podważyłby kluczową dla rozwoju jednolitego rynku zasadę „jednego okienka" i stałby w sprzeczności z fundamentalnym zakazem dwukrotnego karania za ten sam czyn. Ponadto, postępowania prowadzone przez inny niż właściwy zgodnie z art. 51 organ wiązałyby się z dużymi kosztami tłumaczeń i utrudniałyby wyjaśnienie sprawy, zarówno po stronie administratora jak i podmiotu nadzorczego.

b) ad. ust. 2
Wprowadzenie w art. 79 projektu sankcji administracyjnych rodzi możliwości nadużyć i swobody uznania organu nadzoru. Obecnie krajowy nadzorca ochrony danych nie posiada kompetencji do nakładania kary pieniężnej. Proponowany w projekcie sposób nakładania kar odbywa się bez udziału sądu, a katalog naruszeń, za które kara grzywny może być nałożona jest dość szeroki. Analiza tego artykułu prowadzi do wniosku, że grzywna może być nałożona praktycznie za każde naruszenie rozporządzenia. Wątpliwości budzi również wysokość kary, tym bardziej, że wysokość grzywny nie jest ostateczna, ponieważ Komisja Europejska jest uprawniona do przyjmowania aktów mających na celu aktualizację kwoty grzywien administracyjnych, co może naruszać zasadę pewności prawa.

c) ad. ust. 3
Ze względu na potencjalne trudności interpretacyjne związane z wprowadzeniem nowych ram prawnych ochrony danych osobowych, niepewnością związaną z szeroką delegacją dla KE i bardzo wysokimi sankcjami administracyjnymi za naruszenie tych zasad, w opinii Polski kluczowe jest wprowadzenie fazy przejściowej pomiędzy poinformowaniem administratorów i przetwarzających danych o naruszeniu a faktycznym nałożeniem sankcji. Dlatego nałożenie sankcji, powinno poprzedzać ostrzeżenie udzielone przez podmiot nadzorczy wraz ze wskazaniem naruszenia i środków koniecznych do jego naprawienia. Usunięcie naruszenia i współpraca administratora lub podmiotu przetwarzającego powinny być przesłanką zmniejszającą wysokość sankcji. Procedura ostrzegawcza powinna mieć zastosowanie do wszystkich administratorów danych, bez względu na wielkość przedsiębiorstwa.

d) ad. ust. 4-6
Obecny projekt rozporządzenia nakłada na organ ochrony danych obowiązek nałożenia sankcji administracyjnej w określonych przypadkach, natomiast nie daje możliwości odstąpienia od powyższego. Zasadnym jest odejście od obligatoryjności takiego działania i ustanowienie fakultatywności nałożenia kary. Organ badając konkretną sprawę, stopień naruszenia, zawinione działanie podmiotu przetwarzającego dane oraz wszelkie inne okoliczności sprawy miałby możliwość podjęcia decyzji, czy naruszenie jest na tyle istotne, że wymaga nałożenia na podmiot kary, czy też nie. Rozporządzenie w obecnym kształcie takiej możliwości nie daje, co w połączeniu z zaproponowaną wysokością sankcji oraz brakiem jasnych kryteriów jej nakładania jest instrumentem bardzo dotkliwym dla podmiotów przetwarzających dane/ administratorów.

e) ad. ust. 7
Uprawnienie Komisji Europejskiej do przyjmowania aktów delegowanych mających na celu aktualizację kwoty grzywien administracyjnych może naruszać zasadę pewności prawa.

Rozdział IX – Przepisy dotyczące określonych sytuacji związanych z przetwarzaniem danych (art. 80-85)

Dodatkowe informacje do wiadomości delegacji Polskiej:

Analizowane rozporządzenie, gdy wejdzie w życie, uchyli obecnie obowiązującą dyrektywę 95/46/WE3 (art. 88 ust. projektu rozporządzenia oraz motyw 134 preambuły), której implementację stanowią ustawy krajowe, w tym także polska ustawa o ochronie danych osobowych. Z opinii Europejskiego Inspektora Ochrony Danych (EDPS) z dnia 7 marca 2012 r. wynika również, że projekt rozporządzenia precyzyjnie określa w jakim zakresie przepisy krajowe mogą regulować zagadnienia dotyczące przetwarzania i ochrony danych osobowych. Przepisy pozostawią państwom członkowskim możliwość uszczegółowienia i rozwinięcia zasad ustanowionych w rozporządzeniu w przypadku określonych sytuacji związanych z przetwarzaniem danych osobowych (rozdz. IX). W przypadku przepisów o przetwarzaniu danych pracowników w kontekście zatrudnienia (art. 82), nie powinny one naruszać przepisów w zakresie zatrudnienia, a zatem przepisy pozostawałyby komplementarne. Z drugiej strony przepisy w zakresie zdrowia (art. 81), zatrudnienia (art. 82), tajemnicy – przedsiębiorstwa przyp. aut. (art. 84) muszą być ustanowione „w zakresie rozporządzenia" („within the limits of this Regulation"). Nie został określony w projekcie zakres terytorialny tych przepisów. Według interpretacji EDPS takie założenie może zapobiegać derogacjom sektorowym. Sugeruje zatem zamianę tego sformułowania na „without prejudice" czyli „nie narusza".

Artykuł 80 - Przetwarzanie danych osobowych i wolność wypowiedzi
Dotyczy: Artykuł 80 zobowiązuje państwa członkowskie do stosowania wyłączeń i odstępstw od przepisów szczególnych rozporządzenia, o ile jest to konieczne w celu pogodzenia prawa do ochrony danych osobowych z prawem wolności wypowiedzi. Opiera się on na art. 9 dyrektywy 95/46/WE zgodnie z wykładnią Trybunału Sprawiedliwości UE[4].

Uwagi:
Można ewentualnie ponowić pytanie do KE odnośnie znaczenia sformułowań „solely for journalistic purposes Or the purpose of artistic Or literary expression" – czy pod ten opis można zaklasyfikować również np. blogi? (powinny być wyłączone). Wątpliwości bowiem budzi, że sformułowanie jest zbyt wąskie z

[3] 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

[4] Por. w zakresie interpretacji np. wyrok Trybunału Sprawiedliwości UE z dnia 16 grudnia 2008 r., Satakunnan Markkinapörssi i Satamedia (C-73/07, Zb.Orz. z 2008 r., s. I-9831)

punktu widzenia wolności wypowiedzi. Pytanie tego typu zostało już zadane podczas dyskusji na posiedzeniu grupy Przyjaciół Prezydencji 10.01.2013 r. KE wskazuje szersze rozumienie.

Uzasadnienie:
Nadal nie jest jasno określony zakres tego przepisu. Z jednej strony w samym artykule wskazuje się na cele dziennikarskie, wyrazu artystycznego lub literackiego, z drugiej_motyw (121) daje możliwość szerszego rozumienia tego pojęcia „(...) W celu uwzględnienia znaczenia prawa do wolności wypowiedzi w każdym demokratycznym społeczeństwie, należy dokonać wykładni pojęć dotyczących tej wolności, takich jak szeroko rozumiane dziennikarstwo. Państwa członkowskie powinny zatem zaklasyfikować jako działalność „dziennikarską" do celów wyjątków i odstępstw określonych w niniejszym rozporządzeniu, działalność której przedmiotem jest ujawnianie opinii publicznej informacji, opinii lub pomysłów, niezależnie od nośnika wykorzystanego do ich przekazania. Działalność ta nie powinna być ograniczona do agencji medialnych i może być podejmowana zarówno w celach dochodowych, jak i w celach niedochodowych."
Według organizacji konsumenckiej BEUC prawo do ochrony danych nie może być nadużywane, aby ograniczyć wolność wypowiedzi i wolność informacji. EDPS wskazuje, że zagadnienie jest odmiennie regulowane w krajach członkowkich UE, różna jest również linia orzecznicza Europejskiego Trybunału Praw Człowieka RE w Strasburgu. Według EDPS rozwój Internetu sprawił, że prasa nie jest wyłącznym recenzentem życia publicznego, a taką rolę mogą odgrywać blogi. Dotychczasowe wyłączenie „dziennikarskie" ochrony danych z dyrektywy 95/46/WE jest lepsze niż zamiana tego na sformułowanie „w celach dziennikarskich" w projekcie rozporządzenia. EDPS postuluje również dodanie w przepisach, że zarówno prawo do prywatności i wolności wypowiedzi nie mogą być naruszone. Inną kwestią są dane osobowe zawarte w informacji publicznej, także odmiennie regulowane w państwach członkowskich. Stosowne przepisy mogłyby się znaleźć w przepisach rozporządzenia. Mogłby dopuszczać ujawnienie tych danych jeżeli jest to przewidziane prawem krajowym, byłoby to potrzebne do zbilansowania prawa informacji i ochrony danych.

Artykuł 81 - Przetwarzanie danych osobowych dotyczących zdrowia
Dotyczy: Artykuł 81 zobowiązuje państwa członkowskie, z zastrzeżeniem warunków dla szczególnych kategorii danych, do zapewnienia konkretnych gwarancji przy przetwarzaniu na potrzeby świadczenia opieki zdrowotnej. Zgodnie w ww. przepisem, przetwarzanie danych osobowych dotyczących zdrowia musi odbywać się na podstawie prawa Unii lub prawa państwa członkowskiego, które przewiduje odpowiednie i konkretne środki mające na celu zabezpieczenie uzasadnionych interesów podmiotu danych i które są niezbędne m.in. ze względu na interes publiczny w dziedzinie zdrowia publicznego, taki jak ochrona przed poważnymi transgranicznymi zagrożeniami dla zdrowia lub zapewnienie wysokich standardów jakości i bezpieczeństwa, między innymi w przypadku produktów leczniczych lub wyrobów medycznych.

Uwagi:
Delegowany zgłosi wątpliwości dotyczące precyzyjności przepisów zwłaszcza w zakresie wymagań odnośnie zgody na przetwarzanie danych, odpowiedzialności personelu medycznego i wymagań bezpieczeństwa dla sprzętu informatycznego. Należy zadać pytanie do KE o relację z art. 9 ust. 2 (wydaje się, że na jego podstawie można przetwarzać dane dot. zdrowia na podstawie innych niż w art. 81 przesłanek). W art. ust. 2 pkt. h) powinno nastąpić powołanie się także na interes publiczny (przede wszystkim zdrowie publiczne, kwestie epidemiologiczne, zarządzanie i finansowanie ochrony zdrowia, realizacja kontroli itd.). Obecna redakcja wskazanego przepisu (którego jedynie konkretyzacją jest art. 81, do którego się odwołuje) sugeruje, że dane dotyczące zdrowia mogą być przetwarzane jedynie w celu ochrony zdrowia (szczególnie, że nasuwa się interpretacja, że art. 9 ust. 2 pkt h, mówiący o "danych dotyczących zdrowia" wyłącza art. 9 ust. 2 pkt g, jako przepis szczególny; a właśnie w art. 9 ust. 2 pkt g jest mowa o wykonywaniu zadań w interesie publicznym). Uwaga do tłumaczenia - użycie zwrotu "w szczególności" zamiast "taki jak" w art. 81. Katalog działań musi być otwarty, a zastosowanie zwrotu "w szczególności" pozwoli na uniknięcie wątpliwości interpretacyjnych.

a) ad. ust. 1.a)

Pojawia się wątpliwość co do sformułowania w tym przepisie, że dane dotyczące zdrowia "są przetwarzane przez pracownika służby zdrowia podlegającego obowiązkowi zachowania tajemnicy zawodowej lub przez inną osobę również podlegającą równoważnemu obowiązkowi zachowania poufności na podstawie prawa państwa członkowskiego lub przepisów ustanowionych przez właściwe organy krajowe". O ile do niektórych pracowników medycznych (np. lekarz) istnieje regulacja tajemnicy zawodowej (np. lekarskiej), o tyle pojęcie pracownik służby zdrowia obejmuje szeroki krąg osób, które te dane mogą przetwarzać, np. pracownik w rejestracji, recepcji, informatycy itp. Należy postulować zmianę lub doprecyzowanie tego przepisu pod ww. kątem.

b) ad. ust. 1.b)
Nie wydaje się zasadne wskazanie na jedynie "transgraniczne" zagrożenia.

c) ad. ust. 2 w zw. z art. 83
Wydaje się, że przepisy te wpływają na możliwość realizacji projektów w służbie zdrowia (poprzez posłużenie się w art. 81 ust. 2 pojęciami „dokumentacja", „rejestry pacjentów") należy podkreślić te zagadnienia i wyjaśnić zakres regulacji oraz ewentualnie doprecyzować z punktu widzenia możliwości prowadzenia elektronicznej dokumentacji medycznej oraz ogólnie to ujmując elektronizacji dokumentacji zdarzeń medycznych.

d) ad. ust. 3
Przedstawiciel Polski zgłosi propozycję wykreślenia aktu delegowanego, takie kwestie jak: „specifying other reasons of public interest in the area of public health" powinny zostać określone w rozporządzeniu".

Uzasadnienie:
Organizacje konsumenckie sygnalizują możliwość, że dane medyczne mogą być wykorzystywane do marketingu usług medycznych w Interenecie. Dlatego też postulują zakaz technologii trackingu i profilowania na stronach internetowych dotyczących zdrowia. Poważną kwestią jest też zakres podmiotów, który mogłyby/powinny mieć dostęp do takich danych. Czy byłyby to firmy farmaceutyczne, ubezpieczeni? Organizacje konsumenckie mają również wątpliwości jak można rozróżnić dane do celów dokumentacji, statystyki i badań naukowych od danych zdrowotnych dostępnych personelowi medycznemu. Ust. 1a) wskazuje, że przetwarzanie danych może być prowadzone przez inną osobę również podlegającą równoważnemu obowiązkowi zachowania poufności na podstawie prawa państwa członkowskiego lub przepisów ustanowionych przez właściwe organy krajowe. Powinna zostać doprecyzowana w przepisach taka osoba. W opinii EDPS nakładają się przepsiy art. 9 dotyczącym przetwarzania szczególnych kategorii danych osobowych, a art. 81. Ponadto art. 81 nie zabrania przetwarzania przez instytucje prywatne. Jeszcze większe wątpliwości pojawiają się w kontekście transgranicznego przetwarzania danych zdrowotnych (różne są rodzaje zgody na przetwarzanie w państwach członkowskich, agregacja konsultacji medycznych, różne wymagania bezpieczeństwa dla aplikacji eHealth).
Zgodnie z art. 81 ust. 3, Komisja jest uprawniona do przyjmowania aktów delegowanych, zgodnie z art. 86 w celu dalszego określenia innych przesłanek z zakresu interesu publicznego w obszarze zdrowia publicznego, o których mowa ust. 1 lit. b), jak również kryteriów i wymogów dla gwarancji przetwarzania danych osobowych dla celów, o których mowa w ust. 1. W myśl artykułu 290 TFUE akty delegowane to akty prawne o charakterze nieustawodawczym o zasięgu ogólnym. Ich celem jest uzupełnienie lub zmiana innych niż istotne elementów aktów ustawodawczych Rady i Parlamentu Europejskiego.
W tym wypadku wydaje się, iż Komisja może próbować uzupełniać lub zmieniać istotne elementy aktu ustawodawczego przy pomocy aktów delegowanych. „Określenia innych przesłanek z zakresu interesu publicznego w obszarze zdrowia publicznego", jak również „kryteriów i wymogów dla gwarancji przetwarzania danych osobowych dla celów, o których mowa w ust. 1" mogą być istotnymi elementami aktu ustawodawczego.

Artykul 82 - Przetwarzanie w kontekście zatrudnienia

Dotyczy: Artykuł 82 przewiduje uprawnienie państw czlonkowskich do przyjmowania przepisów szczególnych dotyczących przetwarzania danych osobowych w kontekście zatrudnienia. W granicach rozporządzenia państwa członkowskie mogą przyjąć przepisy szczególne regulujące przetwarzanie danych osobowych pracowników w szczególności dla celów procedury rekrutacyjnej, wykonania umowy o pracę, w tym zwolnienia z obowiązków określonych przez przepisy prawa lub przez umowy zbiorowe, zarządzania, planowania i organizacji pracy, bezpieczeństwa i higieny pracy, oraz dla celów wykonywania praw i korzystania ze świadczeń związanych z zatrudnieniem, indywidualnie lub zbiorowo, oraz dla celu zakończenia stosunku pracy (art. 82 ust. 1). Każde państwo członkowskie ma zawiadomić Komisję o przepisach prawa, które przyjęło w ww. zakresie i bezzwłocznie informować o każdej kolejnej zmianie mającej na nie wpływ (art. 82 ust. 2). Jednocześnie Komisja ma być uprawniona do przyjmowania aktów delegowanych w celu dalszego określenia innych warunków i wymogów gwarancji przetwarzania danych osobowych dla celów, o których mowa powyżej (art. 82 ust. 3).

Uwagi:

Wskazane jest rozważenie uzupełnienia katalogu przepisów szczególnych, o których mowa w ust. 1 o sytuację przechowywania danych osobowych w sprawach związanych ze stosunkiem pracy również w okresie po jego ustaniu, ustalonym w prawie krajowym.

Odnosząc się do kwestii przyznania Komisji Europejskiej prawa do wydawania aktów delegowanych w zakresie spraw związanych z zatrudnieniem, powstaje pytanie o zasadność tego rodzaju delegowania uprawnień (w szczególności, jakich warunków mialoby to dotyczyć).

Ponadto, wymaga zwrócenia uwagi regulacja instytucji „zgody", jako podstawy zgodnego z prawem przetwarzania danych osobowych. W świetle art. 7 ust. 4 projektu zgoda nie stanowi podstawy prawnej przetwarzania danych osobowych w sytuacji poważnej nierówności między podmiotami danych a administratorem. W motywie 34 preambuły rozporządzenia wyjaśniono, iż dotyczy to w szczególności przetwarzania danych osobowych pracowników przez pracodawców. Tym samym zgoda pracownika nie będzie mogła stanowić samoistnej podstawy do przetwarzania danych osobowych przez pracodawcę. W tym kontekście wymaga zbadania kwestia dopuszczalności praktyki dobrowolnego ujawniania lub przekazywania, przez osobę ubiegającą się o zatrudnienie bądź pracownika, informacji wychodzących poza zakres wyraźnie wskazany obecnie w przepisach.

Ponadto delegat może poinformować o konieczności utrzymania „dobrze sprawdzających się" polskich szczególnych rozwiązań dotyczących ochrony danych pracowników w Kodeksie pracy, na co zwracała uwagę Senacka Komisja Praw Człowieka, Sprawiedliwości i Petycji w swej opinii co do pakietu oraz jej przewodniczący Pan Prof. Seweryński podczas swego wystąpienia w czasie Międzyparlamentarnej Sesji LIBE w Parlamencie Europejskim.

Dodatkowe informacje do wiadomości delegacji Polskiej:

Według think tanku Brussels European Employee Relations Group reprezentujących pracodawców w UE, Stanach Zjednoczonych, Indiach i Japonii pozostawienie w art. 82 rozporządzenia możliwości przyjęcia przez państwa członkowskie wlasnych regulacji dotyczących przetwarzania danych osobowych może ograniczyć korzyści jakie niesie rozporządzenie i może generować koszty, które na podstawie wstępnych szacunków mogą wynosić około 3 miliardów € rocznie5. Nowe rozwiązanie może oznaczać zachowanie „status quo" wraz z nowymi wymaganiami wynikającymi z obecnego rozporządzenia, w tym kosztów zatrudnienia inspektorów ochrony danych w dużych przedsiębiorstwach.

Z uwagi na kompleksowość aktu prawnego istotne znaczenie dla oceny art. 82 przez MPiPS miałaby możliwość zapoznania się ze stanowiskiem organu wiodącego i GIODO nt. potencjalnego wpływu rozporządzenia na dotychczasowe rozwiązania krajowe.

[5] Na podstawie informacji z http://www.euractiv.com. Szacunek powstał z analizy, że koszty dla 40 tys. dużych przedsiębiorstw europejskich, które prowadzi rocznie średnio trzy projekty z zakresu przetwarzania danych pracowników to 2,2 miliarda €, a pozostałe koszty odnoszą się do małych i średnich przedsiębiorstw.

Artykuł 83 - Przetwarzanie do celów dokumentacji, statystyki i badań naukowych
Dotyczy: Artykuł 83 określa szczególne warunki przetwarzania danych osobowych do celów dokumentacji, statystyki i badań naukowych.

Uwagi:
Pyt. do KE o definicję „statistical purposes", sugestia ograniczenia wyłączeń do celów statystycznych jedynie w zakresie statystyki publicznej. Prośba o wyjaśnienie zależności i powiązań pomiędzy art. 83 a art. 9 ust 2 (sytuacja podobna jak w przyp. art. 81). Sugestia wykreślenia odwolania do aktu delegowanego (ust.3).
Wskazanie na wątpliwości zgłaszane przez polski GUS dotyczące art. 83 (sugestia wykreślenia ust.1 lit.b – którego zapisy uniemożliwialoby prawidlowe funkcjonowanie statystyki publicznej).
Należy też zwrócić uwagę na nieprecyzyjny charakter przepisu ujętego w art.83 ust.1. Z przepisu tego wnioskować można, że podmiot wnioskujący o dane statystyczne, dane przetwarzane w celach badań naukowych, dane przetwarzane w celach dokumentacji, zobowiązany bylyby najpierw do wykorzystania możliwość uzyskania zanonimizowanych danych z innych źródeł (badań naukowych, publikacji, innych źródeł dysponujących już zanonimizowanymi danymi). Obecnie obowiązujące przepisy nie wymagają podejmowania takich działań.

Uzasadnienie:
Główny Urząd Statystyczny wskazuje na konieczność wprowadzenia do projektu rozporządzenia zmian uwzględniających wymogi umożliwiające prawidłowe funkcjonowanie statystyki publicznej. Dotyczy to w szczególności art. 6. 14, 15, 16, 18 oraz 83. Wnioskuje o usunięcie przepisów uprawniających Komisję do wydawania aktów delegowanych w kwestiach związanych z „celami statystycznymi". Wynika to z następujących przyczyn:
- wprowadzenie aktów delegowanych może skutkować nałożeniem na państwa członkowskie obowiązków statystycznych, których nie będą mogly zrealizować w wyniku braku odpowiedniego przygotowania metodologicznego, nadmiernego obciążenia administracyjnego, ich uregulowań wewnętrznych lub też z innych przyczyn wynikających zwlaszcza z panującego kryzysu finansowego,
- proponowana delegacja dotyczy praw i obowiązków takich jak: ograniczanie informacji statystycznych, precyzowanie warunków dostępu do danych. Kwestie te mogą być istotnymi elementami aktu ustawodawczego i powinny zostać uregulowane w akcie podstawowych (rozporządzeniu).
W kwestiach precyzyjności przepis art. 83 ust. 1 lit. a nie precyzuje na kim spoczywałby ciężar udowodnienia, że podmiot podjął wszelkie czynności zmierzające do uzyskania tych danych. Jeżeli ciężar dowodu spoczywałby na organie, wówczas konieczne byłoby prowadzenie postępowań wyjaśniających, co byłoby uciążliwe dla administratorów zbiorów wielkoskalowych. Rozwiązanie takie budzi poważne wątpliwości co do zasadności jego przyjęcia, jak się wydaje należy dążyć do poszukiwania rozwiązań w tym zakresie, które zmniejszylyby obciążenia administratorów wielkoskalowych (publicznych) zbiorów danych.
Mając na uwadze powyższe, należy poprzeć tekst art. 83 w brzmieniu zaproponowanym w piśmie przewodniczącego Grupy Roboczej ds. Statystyki (CWPS) skierowanym do Grupy DAPIX. W rezultacie, utrzymany zostałby paragraf 1 oraz paragraf 2 (z wyjątkiem lit. b, której utrzymanie uniemożliwiłoby prawidłowe funkcjonowanie statystyki publicznej). W miejsce paragrafu 3 dotyczącego aktów delegowanych dołączony zostałby paragraf 1A, zapewniający dodatkowe gwarancje bezpieczeństwa dla podmiotu danych, w sytuacjach gdy ochrona tych danych byłaby wyłączona mając na uwadze cele statystyczne (propozycje zmian art. 14, 15, 16, 18).

Dodatkowe informacje do wiadomości delegacji Polskiej:
Sporną kwestią jest fakt czy dane statystyczne zbierane w ramach statystyki europejskiej poddane są innemu niż dane osobowe reżimowi prawnemu, znajdującemu swe źródlo w TFUE (art. 16 - zapewniający ochronę danych osobowych wobec art. 338 dotyczącego statystyki). Europejski Inspektor Ochrony Danych zwraca uwagę na zamianę sformułowania „w granicach niniejszego rozporządzenia" na „bez uszczerbku dla przepisów niniejszego rozporządzenia". W opinii Rady Legislacyjnej przy Prezesie Rady Ministrów DP-10-20(3) z 6 września 2012 r. dotyczącej przetwarzania danych osobowych w programie statystyki publicznej na rok 2013, która w cz. IV - szczególnie w akapicie 3 i 4 na str. 10 i 11 – opisuje wzajemny stosunek art.

16 i 338 TFUE, zaś w akapicie I. (str. 9) tejże cz. IV wskazuje na poprawny sposób interpretacji rozporządznia 223/2009.

Artykul 84 - Obowiązki dotyczące zachowania tajemnicy
Dotyczy: Artykuł 84 upoważnia państw czlonkowskie do przyjmowania przepisów szczególnych dotyczących dostępu organów nadzorczych do danych osobowych i pomieszczeń, w których administratorzy podlegają obowiązkowi zachowania tajemnicy.

Uwagi:
Brak uwag.

Artykul 85 - Obowiązujące przepisy dotyczące ochrony danych stosowane przez kościoły i związki wyznaniowe
Dotyczy: Artykul 85 umożliwia, w świetle art. 17 Traktatu o funkcjonowaniu Unii Europejskiej, nieprzerwane stosowanie obowiązujących kompleksowych przepisów dotyczących ochrony danych kościołów, jeśli zostaly one ujednolicone z przepisami rozporządzenia.

Uwagi:
Delegowany zapozna się z komentarzami innych państw członkowskich. W opinii GIODO jak i KE (odp. na grupie Przyjaciól Prezydencji) przepis nie jest kontrowersyjny i dotyczy regulacji z zakresu ochrony danych, które są stosowane przez kościoły i związki wyznaniowe. Państwa członkowskie wskazują jednak na małą elastyczność przepisu.

Dodatkowe informacje do wiadomości delegacji Polskiej:
Zgodnie z opinią GIODO art. 85 projektu rozporządzenia dotyczy ochrony danych osobowych w kościołach i związkach wyznaniowych w krajach w których istnieje kompleksowe rozwiązanie w tym sektorze. Takim krajem są np. Niemcy i do nich odnosi się ten przepis przejściowy. Polska nie posiada takiego rozwiązania prawnego i albo powinna je stworzyć, albo nie ma powodu by wnosić uwagi do tego artykulu.

Rozdział X – AKTY DELEGOWANE I WYKONAWCZE

Uwagi:
PL ma wątpliwości odnośnie uprawnień Komisji do wydawania aktów delegowanych i wykonawczych. PL nie wyklucza co prawda istnienia uzasadnienia dla uprawnień Komisji do regulowania pewnych kwestii w formie aktów delegowanych (w niektórych przypadkach odwołanie do aktów delegowanych jest uzasadnione), jednak projekt rozporządzenia przewiduje ich zbyt dużą liczbę. Polska zgadza się, że akty delegowane powinny ograniczać się do regulowania „innych niż istotne" elementów aktu ustawodawczego - stosownie do postanowień art. 290 TFUE.
PL przekaże szczególowe uwagi dot. aktów delegowanych na późniejszym etapie. Wskazane jest przeprowadzenie przedtem pogłębionej dyskusji nt. możliwych alternatyw zastepujących akty delegowane, tak jak to zostalo wskazane w dokumencie podsumowującym prace podczas PREZ CY. Czy PREZ IE zamierza wrócić do szczegółowej dyskusji w zakresie aktów delegowanych i wykonawczych?

ROZDZIAŁ XI - PRZEPISY KOŃCOWE

Artykul 91 Wejście w życie i stosowanie
Dotyczy: Artykuł 91 określa datę wejścia w życie rozporządzenia oraz okres przejściowy przed datą rozpoczęcia jego stosowania.

Uwagi:
Delegowany zapozna się z komentarzami innych państw członkowskich.

Uzasadnienie:
Zgodnie z opiniami interesariuszy z sektora finansowego określony w art. 91 dwuletni termin stosowania rozporządzenia od dnia wejścia w życie jest zbyt krótki biorąc pod uwagę wymagania dotyczące dostosowania środków technicznych do wymogów zawartych obecnie w Rozporządzeniu (zmiany w systemach bankowych). W opinii GIODO dwuletni termin na dostosowanie systemów teleinformatycznych do wymagań rozporządzenia jest wystarczający. Biorąc po uwagę aktualny rozwój systemów nie widać uzasadnienia dla jego wydłużania. Systemy teleinformatyczne poddawane są fundamentalnym zmianom w terminach o wiele krótszych. Nie wskazano również, które z proponowanych w rozporzadzeniu zmian miałby wymagać znacznej modernizacji systemów bankowych. O ile pewnym wyzwaniem może być przegląd dokumentacji istniejących systemów pod kątem oceny, czy dokumentacja ta spełnia ewnetualne wymagania rozporządzenia, o tyle trudno dostrzec jakiekolwiek problemy w zakresie przebudowy „systemów bankowych".

Sporządził: Jarosław Łuba, DSI MAiC (przy wykorzystaniu wkładów GIODO, MS, MSW, GUS, MZ, MPiPS)

Akceptował: Maciej Groń, Dyrektor Departamentu Społeczeństwa Informacyjnego MAiC

DYREKTOR
DEPARTAMENTU SPOŁECZEŃSTWA INFORMACYJNEGO
MINISTERSTWA ADMINISTRACJI I CYFRYZACJI
Maciej GROŃ

Data: 28 stycznia 2013 r.