

KIERUNKI ZMIAN W EUROPEJSKIM PRAWIE DOTYCZĄCYM OCHRONY DANYCH OSOBOWYCH I ICH WPŁYW NA SEKTOR BANKOWY

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

Warszawa, 13 lutego 2013 r.

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

TRAKTATOWA PODSTAWA DO OCHRONY DANYCH OSOBOWYCH

Artykuł 16 Traktatu o funkcjonowaniu UE (po zm. z Lizbony)

1. Każda osoba ma prawo do ochrony danych osobowych jej dotyczących.
2. Parlament Europejski i Rada, stanowiąc zgodnie ze zwykłą procedurą ustawodawczą, określają zasady dotyczące ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii oraz przez Państwa Członkowskie w wykonywaniu działań wchodzących w zakres zastosowania prawa Unii, a także zasady dotyczące swobodnego przepływu takich danych. Przestrzeganie tych zasad podlega kontroli niezależnych organów.

Zasady przyjęte na podstawie niniejszego artykułu pozostają bez uszczerbku dla zasad szczególnych przewidzianych w artykule 39 Traktatu o Unii Europejskiej.

PODSTAWA DO OCHRONY DANYCH OSOBOWYCH W OBECNYM PRAWIE UE

Podstawowy dokument ustanawiający obowiązujące unijne przepisy o ochronie danych, dyrektywa 95/46/WE¹, został przyjęty w 1995 r. z myślą o realizacji dwóch celów: ochrony podstawowego prawa do ochrony danych oraz zagwarantowania swobodnego przepływu danych między państwami członkowskimi

Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dz.U. L 281 z 23.11.1995, s. 31.

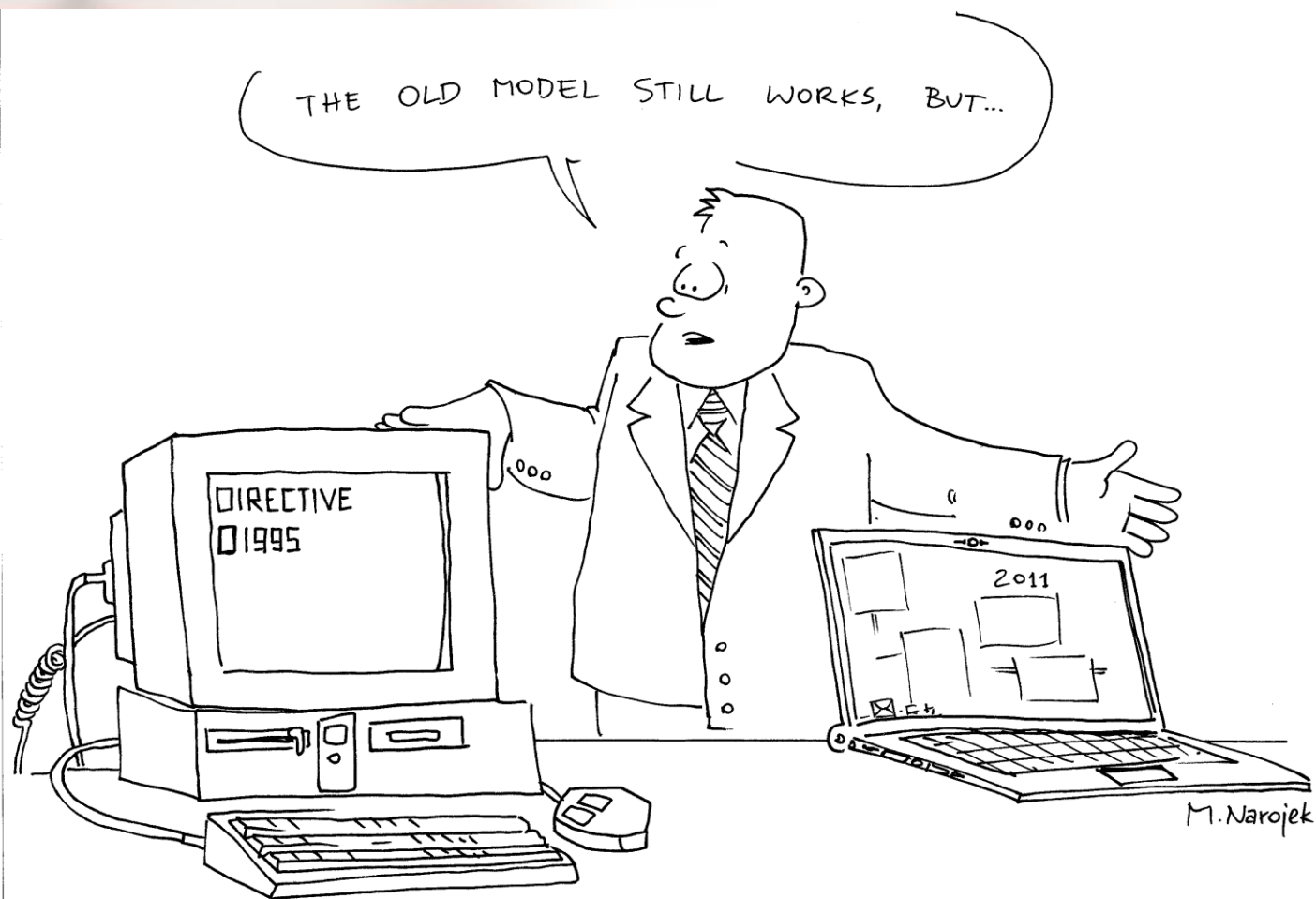
Została ona uzupełniona przez szereg instrumentów przewidujących przepisy szczególne o ochronie danych w obszarze współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych (były trzeci filar), w tym **decyzję ramową 2008/977/WSiSW Rady 2008/977/WSiSW z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych, Dz.U. L 350 z 30.12.2008, s. 60.**

ZMIANA RAM PRAWNYCH OCHRONY DANYCH OSOBOWYCH W EUROPIE I W POLSCE

**KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO,
RADY, EUROPEJSKIEGO KOMITETU EKONOMICZNO-
SPOŁECZNEGO ORAZ KOMITETU REGIONÓW**

**„Całościowe podejście do kwestii ochrony danych osobowych
w Unii Europejskiej”**

ZMIANA RAM PRAWNYCH OCHRONY DANYCH OSOBOWYCH W EUROPIE I W POLSCE



ZMIANA RAM PRAWNYCH OCHRONY DANYCH OSOBOWYCH W EUROPIE I W POLSCE

**Projekt rozporządzenia Parlamentu Europejskiego i Rady
w sprawie
ochrony osób fizycznych w zakresie przetwarzania danych
osobowych i swobodnego przepływu tych danych
COM(2012) 11 z 25 stycznia 2012 r.**

ZMIANA RAM PRAWNYCH OCHRONY DANYCH OSOBOWYCH W EUROPIE I W POLSCE

Projekt dyrektywy Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy w celu zapobiegania, dochodzenia, wykrywania lub ścigania przestępstw lub wykonywania sankcji karnych i swobodnego przepływu tych danych

COM(2012) 10 z 25 stycznia 2012 r.

ZMIANA RAM PRAWNYCH OCHRONY DANYCH OSOBOWYCH W EUROPIE I W POLSCE



Christopher Kuner,
The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law, Privacy and Security Law Report, BNA Bloomberg
6 February 2012,
s. 1-15

ZMIANA RAM PRAWNYCH OCHRONY DANYCH OSOBY W EUROPIE I W POLSCE

Rozporządzenie

+

Dyrektywa

PRZEBIEG PRAC

Rada Europejska

Grupa roboczej Rady UE ds. Wymiany Informacji i Ochrony Danych

Polskę reprezentują:

Ministerstwo Administracji i Cyfryzacji i/lub
Ministerstwo Spraw Wewnętrznych oraz
Stałe Przedstawicielstwo RP przy UE

Eksperci uczestniczący w Grupie:

Biuro Generalnego Inspektora Ochrony Danych Osobowych

Stanowisko Polski uzgadniają: Ministerstwo Gospodarki, Ministerstwo Sprawiedliwości, Ministerstwo Zdrowia, Główny Urząd Statystyczny, Urząd Komunikacji Elektronicznej oraz Ministerstwo Spraw Zagranicznych

Instrukcję przyjmuje:

Komitet Rady Ministrów ds. UE

•

PRZEBIEG PRAC

Parlament Europejski



Sprawozdawcy PE:

Jan Philipp Albrecht (D – Zieloni) – rozporządzenie

Dimitrios Droutsas (GR – Socjaliści) – dyrektywa

PRZEBIEG PRAC

Parlament Europejski Mapa drogowa Jana Philippa Albrechta

- Wrzesień 2012: Wymiana poglądów nt. rozporządzenia w komisji LIBE
- 9-10 października 2012 - *Komitet Międzyparlamentarny Parlamentu Europejskiego i parlamentów krajowych (Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych LIBE)*
- Październik 2012: Prezentacja szczegółowego dok. roboczego nt. rozporządzenia (WD 2)
- Październik /listopad 2012: Czytanie w komisji LIBE
- Listopad 2012: Prezentacja projektu sprawozdania
- Grudzień 2012: Termin wnoszenia poprawek
- Koniec stycznia/luty 2013: Dyskusja nt. poprawek w Komisji LIBE
- Luty 2013: Dyskusja nt. opinii innych komisji
- Marzec/kwiecień 2013: Orientacyjne głosowanie w LIBE
- Lato 2013 (?) Trylog z Radą i Komisją
- Początek 2014 (?): Głosowanie na sesji plenarnej

PRZEBIEG PRAC

9-10 października 2012
Komitet Międzyparlamentarny
Parlamentu Europejskiego
i parlamentów krajowych
(Komisja Wolności Obywatelskich,
Sprawiedliwości i Spraw
Wewnętrznych LIBE)

**The reform of the EU Data
Protection framework
"Building trust in a digital
and global world"**

INTERPARLIAMENTARY COMMITTEE MEETING
Committee on Civil Liberties, Justice and Home Affairs
European Parliament - National Parliaments

The Reform of the EU Data Protection Framework

Building Trust in a Digital and Global World

Chaired by
Juan Fernando LÓPEZ AGUILAR
Chair of the Committee
on Civil Liberties, Justice
and Home Affairs

Opening speeches by
Martin SCHULZ
President of the European Parliament
and **Viviane REDING**
Vice-President of the European Commission

Tuesday 9 > 09.00 - 18.30
Wednesday 10 > 09.00 - 18.30
October 2012
József Antall Building
Room JAN 402
European Parliament
Brussels

DE ITIC, ECIT Directorate | Designed by CLIENTS AND PROJECTS OFFICE, Internet Service Unit | Printed by Printing Units

With the support of the Directorate for
Relations with National Parliaments

EUROPEAN PARLIAMENT

PRZEBIEG PRAC

LIBE - 10 January 2013,

5. Protection of individuals with regard to the processing of personal data, and the free movement of such data (General Data Protection Regulation)

Rapporteur Jan Philipp Albrecht (Verts/ALE)

PR – [PE501.927v02-00](#)

DT – [PE497.803v02-00](#)

DT – [PE497.802v01-00](#)

DT – [PE491.322v01-00](#)

EMPL – Nadja Hirsch (ALDE) PA – [PE498.045v01-00](#) AM – [PE500.581v01-00](#)

ITRE – Seán Kelly (PPE) PA – [PE496.562v01-00](#) AM – [PE502.053v01-00](#)

IMCO – Lara Comi (PPE) PA – [PE496.497v01-00](#) AM – [PE500.411v01-00](#)

JURI – Marielle Gallo (PPE) PA – [PE494.710v01-00](#) AM – [PE500.695v01-00](#)

- Decision on deadline for tabling amendments
- Deadline for tabling amendments: **27 February 2013, 12.00**

ZMIANA RAM PRAWNYCH OCHRONY DANYCH OSOBOWYCH W EUROPIE I W POLSCE

Bezpośrednie obowiązywanie

Bezpośrednie stosowanie

Bezpośredni skutek

norm prawa europejskiego w dyrektywie i w rozporządzeniu

ZMIANA RAM PRAWNYCH OCHRONY DANYCH OSOBOWYCH W EUROPIE I W POLSCE

Jurysdykcja

Prawo właściwe

ZMIANA RAM PRAWNYCH OCHRONY DANYCH OSOBOWYCH W EUROPIE I W POLSCE

Procedury koordynacyjne

ZMIANA RAM PRAWNYCH OCHRONY DANYCH OSOBOWYCH W EUROPIE I W POLSCE

Rola Komisji Europejskiej

ZMIANA RAM PRAWNYCH OCHRONY DANYCH OSOBOWYCH W EUROPIE I W POLSCE

Koniec z notyfikacją w starym stylu

ZMIANA RAM PRAWNYCH OCHRONY DANYCH OSOBOWYCH W EUROPIE I W POLSCE

Wrażliwe przetwarzanie (*risky processing*)

zamiast

ochrony danych wrażliwych

ZMIANA RAM PRAWNYCH OCHRONY DANYCH OSOBOWYCH W EUROPIE I W POLSCE

Ujednolicenie zasad wdrażania prawa przez organy ochrony danych

ZMIANA RAM PRAWNYCH OCHRONY DANYCH OSOBOWYCH W EUROPIE I W POLSCE

Pozycja ustrojowa, finansowa i organizacyjna organów ochrony danych

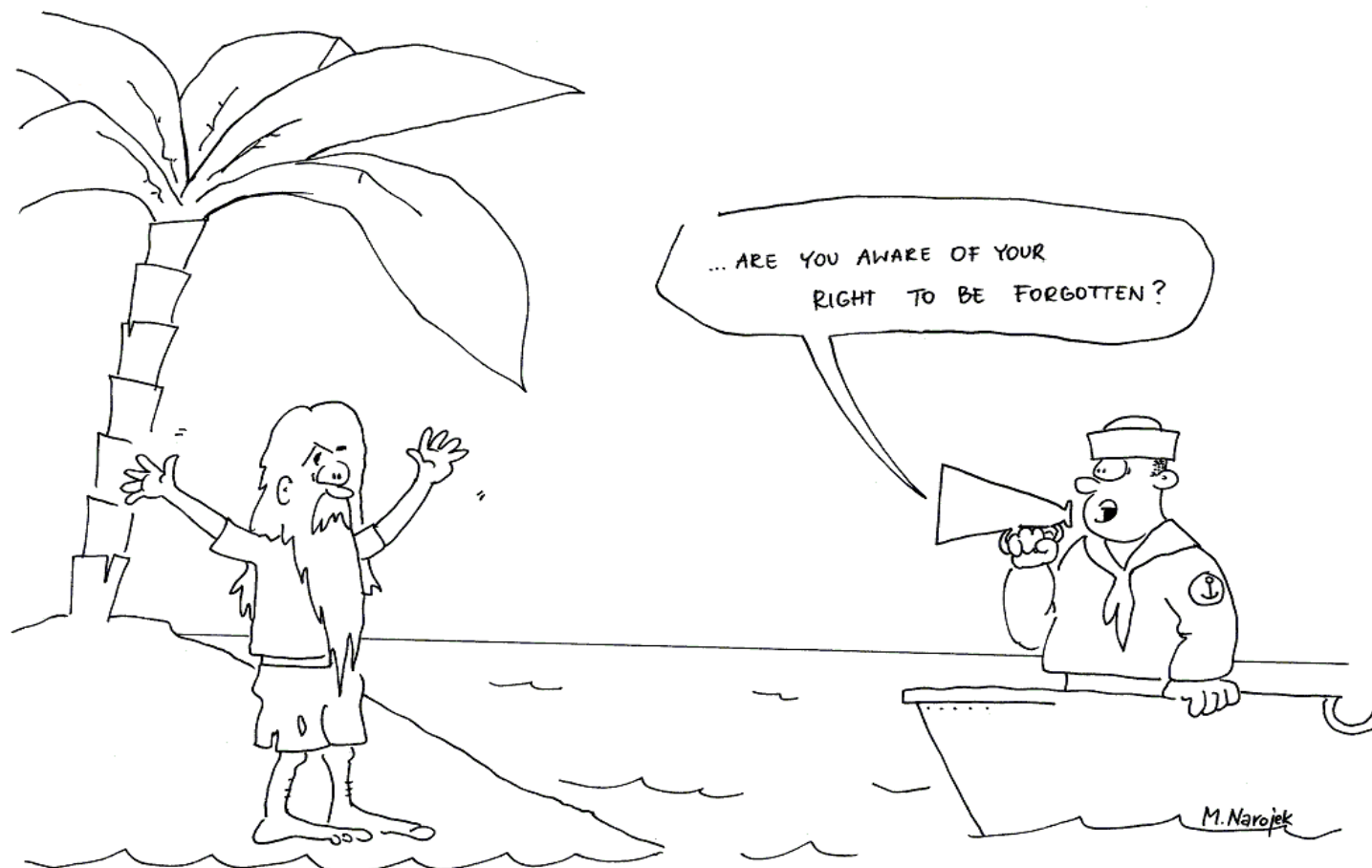
ZMIANA RAM PRAWNYCH OCHRONY DANYCH OSOBY W EUROPIE I W POLSCE

Wyrażna zgoda
(*explicit consent*)

ZMIANA RAM PRAWNYCH OCHRONY DANYCH OSOBOWYCH W EUROPIE I W POLSCE

Obowiązkowy administrator bezpieczeństwa informacji
(data protection officer)

ZMIANA RAM PRAWNYCH OCHRONY DANYCH OSOBOWYCH W EUROPIE I W POLSCE



ZMIANA RAM PRAWNYCH OCHRONY DANYCH OSOBOWYCH W EUROPIE I W POLSCE

Privacy by design

Privacy impact assessments

ZMIANA RAM PRAWNYCH OCHRONY DANYCH OSOBOWYCH W EUROPIE I W POLSCE

Ujednolicenie zasad przetwarzania danych osobowych w Policji i wymiarze sprawiedliwości

**Realizacja zasad ochrony danych wynikających z prawa europejskiego również przy „przetwarzaniu krajowym”
(*domestic processing*)**

KONTROWERSJE

Artykuł 6 Zgodność z prawem przetwarzania

1. Przetwarzanie danych osobowych jest zgodne z prawem, o ile ma zastosowanie co najmniej jeden z poniższych elementów:
 - a) podmiot danych wyraził zgodę na przetwarzanie swoich danych osobowych do jednego lub większej liczby konkretnych celów;
 - b) przetwarzanie danych jest konieczne do wykonania umowy, której stroną jest podmiot danych, lub w celu podjęcia działań na żądanie podmiotu danych przed zawarciem umowy;
 - c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
 - d) przetwarzanie jest konieczne w celu ochrony żywotnych interesów podmiotów danych;
 - e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub wykonania władzy publicznej powierzonej administratorowi;
 - f) przetwarzanie jest konieczne dla celów wynikających ze słuszych interesów realizowanych przez administratora, z wyjątkiem sytuacji, kiedy nadrzędny charakter ma interes podstawowych praw i wolności podmiotu danych, które wymagają ochrony danych osobowych, w szczególności gdy podmiotem danych jest dziecko. Przepisu tego nie stosuje się do przetwarzania realizowanego przez organy publiczne w wykonaniu ich zadań.

KONTROWERSJE

Artykuł 6 **Zgodność z prawem przetwarzania** (...)

2. Przetwarzanie danych osobowych, konieczne do celów dokumentacji, statystyki lub badań naukowych, jest zgodne z prawem, z zastrzeżeniem warunków i gwarancji, o których mowa w art. 83.
3. Podstawa przetwarzania, o której mowa w ust. 1 lit. c) i e), musi być przewidziana w:
 - a) prawie Unii; lub
 - b) prawie państwa członkowskiego, któremu podlega administrator.Prawo państwa członkowskiego musi realizować cel leżący w interesie publicznym lub musi być konieczne do ochrony praw i wolności innych osób, respektować istotę prawa do ochrony danych osobowych i być proporcjonalne do wyznaczonego słusznego celu.
4. Jeśli cel dalszego przetwarzania nie jest zgodny z celem, dla którego zebrano dane osobowe, przetwarzanie musi opierać się na co najmniej jednej z podstaw prawnych przewidzianych w ust. 1 lit. a)-e). Ma to w szczególności zastosowanie do każdej zmiany ogólnych warunków umowy.
5. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 86 w celu doprecyzowania warunków, o których mowa w ust. 1 lit. f), dla różnych sektorów i sytuacji, w których przetwarza się dane, w tym jeśli chodzi o przetwarzanie danych osobowych dotyczących dziecka.

KONTROWERSJE

Artykuł 9 Przetwarzanie szczególnych kategorii danych osobowych

1. Zakazuje się przetwarzania danych osobowych ujawniających rasę lub pochodzenie etniczne, poglądy polityczne, religię lub przekonania, przynależność do związków zawodowych oraz przetwarzania danych genetycznych lub danych dotyczących zdrowia lub seksualności, wyroków skazujących lub powiązanych środków zabezpieczających.
2. Ustęp 1 nie ma zastosowania, w przypadku gdy:
 - a) podmiot danych udzielił zgody na przetwarzanie tych danych osobowych, z zastrzeżeniem warunków określonych w art. 7 i 8, z wyjątkiem sytuacji, gdy prawo Unii lub prawo państwa członkowskiego przewiduje, że zakaz, o którym mowa w ust. 1, nie może być uchylony przez podmiot danych; lub
 - b) przetwarzanie danych jest konieczne do celów wypełniania obowiązków i wykonania szczególnych uprawnień administratora w dziedzinie prawa pracy, o ile jest to dozwolone przez prawo Unii lub prawo państwa członkowskiego przewidujące odpowiednie gwarancje; lub
 - c) przetwarzanie jest niezbędne w celu ochrony żywotnych interesów podmiotu danych lub innej osoby, w przypadku gdy podmiot danych nie jest fizycznie lub prawnie zdolny do wyrażenia zgody;

KONTROWERSJE

Artykuł 9 Przetwarzanie szczególnych kategorii danych osobowych

(...)

- e) przetwarzanie dotyczy danych osobowych, które zostały wyraźnie podane do publicznej wiadomości przez podmiot danych; lub
- f) przetwarzanie jest niezbędne do ustalenia, realizacji lub ochrony roszczeń prawnych; lub
- g) przetwarzanie jest niezbędne do wykonania zadania w interesie publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie środki ochrony słuszných interesów podmiotu danych; lub (...)
- i) przetwarzanie jest niezbędne do celów dokumentacji, statystyki lub badań naukowych, z zastrzeżeniem warunków i gwarancji, o których mowa w art. 83; lub
- j) przetwarzanie danych dotyczących wyroków skazujących za przestępstwa lub powiązanych środków zabezpieczających odbywa się pod kontrolą oficjalnego organu lub przetwarzanie jest niezbędne dla wypełnienia obowiązku prawnego lub regulacyjnego, któremu podlega administrator, albo w celu wykonania zadania realizowanego w ważnym interesie publicznym, o ile jest to dozwolone na mocy prawa Unii lub prawa państwa członkowskiego przewidującego odpowiednie gwarancje. Kompletny rejestr wyroków skazujących za przestępstwa jest prowadzony wyłącznie pod nadzorem oficjalnego organu.

KONTROWERSJE

„Profil” oznacza zestaw danych charakteryzujący kategorię osób, który ma zostać zastosowany odniesieniu do danej osoby.

„Tworzenie profili” oznacza automatyczną technikę przetwarzania danych polegającą na przypisaniu danej osobie „profilu” w celu podejmowania dotyczących jej decyzji bądź analizy lub przewidywania jej preferencji, zachowań i postaw.



KONTROWERSJE

Tworzenie profili, wg Grupy art. 29

Istnieją dwa podstawowe podejścia do tworzenia profili użytkowników:

*i) **Profile predykcyjne*** tworzy się w drodze wnioskowania na podstawie obserwacji indywidualnego i zbiorowego zachowania użytkowników w czasie, w szczególności poprzez monitorowanie odwiedzanych stron oraz reklam, które użytkownik wyświetla, lub na które klika.

*ii) **Profile jawne*** tworzy się na podstawie danych osobowych przekazywanych w ramach usługi sieciowej przez same osoby, których dane dotyczą, np. podczas rejestracji. Wspomniane podejścia można łączyć. Ponadto profile predykcyjne mogą stać się jawne później, kiedy osoba, której dotyczą dane utworzy dane logowania dla danej strony internetowej.

Patrz: Opinia Grupy art. 29 nr 2/2010 w sprawie internetowej reklamy behawioralnej przyjęta dnia 22 czerwca 2010 r., pkt 2.3., str. 8

KONTROWERSJE

Profilowanie – 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 sytuację osoby;

Przepis w sposób wyraźny odwołuje się do wskazań zawartych w rekomendacji CM/Rec (2010) 13 przyjętej przez Komitet Ministrów Rady Europy w dniu 23.11.2010 r. podczas 1099. posiedzenia wiceministrów
<https://wcd.coe.int/wcd/ViewDoc.jsp?id=1710949&Site=CM>.

KONTROWERSJE

Profilowanie - W projekcie pojawiły się również zakazy i ograniczenia dotyczące profilowania (art. 20 projektu rozporządzenia). (...) Profilowaniem nazywamy dwie grupy czynności podejmowanych przez przetwarzającego dane. W pierwszej zbierane są dane z różnych źródeł, o których wiadomo, że dotyczą tej samej zidentyfikowanej osoby. Jest to więc operacja obejmująca zespół technik *data miningu* dokonywana na zbiorach, w których przetwarzamy dane, co do których mamy silne podstawy by sądzić, że dotyczą one tej samej osoby i są one wystarczająco dobrej jakości, by wspólnie tworzyć wartość dodaną.

W drugim rozumieniu profilowanie odnoszone do pojedynczej osoby polega na wnioskowaniu o cechach nieznanych dla data minera z cech przypisanych już wcześniej danej osobie. Ta metoda obejmuje zazwyczaj tworzenie profili grupowych, w których gromadzone są cechy wielu osób, umożliwiając statystyczne wnioskowanie o występowaniu cechy, której u danej osoby nie znamy, na podstawie przynależności tej osoby do populacji wykazującej te same cechy, które u danej osoby już rozpoznaliśmy.

W.R.Wiewiórowski: *Nowe ramy ochrony danych osobowych w Unii Europejskiej*, Monitor Prawniczy - Dodatek 'Ochrona danych osobowych' [red:] G. Sibiga, Nr 7/2012, s. 1-8

KONTROWERSJE

Profilowanie - Metoda uzupełniania zestawu cech osobowych o cechy, których występowania nie jesteśmy pewni, ale których możemy się na podstawie analizy danych statystycznych spodziewać jest szczególnie niebezpieczna z punktu widzenia ochrony prywatności. O ile bowiem w pierwszym z opisanych przypadków mamy do czynienia z zestawianiem cech, które zdaniem przetwarzającego są prawdziwe dla danej osoby, o tyle w drugim przypadku nawet przetwarzający uznaje możliwość istnienia błędu w opisie osoby, ale uznaje – racjonalnie lub nie – że błąd taki może pominąć. Pierwsza z metod ingeruje więc przede wszystkim w autonomię informacyjną osoby powodując, że dane na jej temat zestawiane są ponad standard jaki wynika z prawa i ponad zakres na jaki osoba się zgodziła. Druga z metod zaś prowadzi wprost do tworzenia profili nieprawdziwych, przy których dla oceny przetwarzającego błąd nie jest znaczący. Takie postępowanie rodzi duże zagrożenie naruszenia podstawowych praw i wolności obywateli, a w szczególności prawa rodzi niebezpieczeństwo dyskryminacji ze względu na płeć, pochodzenie etniczne i rasowe, wyznanie i przekonania, niepełnosprawność, wiek czy orientację seksualną, które zwiększane jest zakładaną przez przetwarzającego niedokładnością danych.

W.R.Wiewiórowski: *Nowe ramy ochrony danych osobowych w Unii Europejskiej*, Monitor Prawniczy - Dodatek 'Ochrona danych osobowych' [red:] G. Sibiga, Nr 7/2012, s. 1-8

KONTROWERSJE

Profilowanie - Oba opisane wyżej procesy nie muszą być rozłączne, można nawet zaryzykować stwierdzenie, że drugi z procesów jest z reguły poprzedzany przez pierwszy, jako że wnioskowanie o danych statystycznie prawdziwych jest szczególnie przydatne w sytuacji, gdy danych pewnych jest wiele i gdy można na nich przeprowadzać wielorakie symulacje, co do przynależności osoby do grup wzorcowych.

W części opracowań dotyczących profilowania uznaje się, że z pełnym profilowaniem mamy do czynienia jedynie wówczas, gdy na podstawie danych uznawanych za prawdziwe i/lub danych „statystycznie prawdziwych” tworzy się wzorce zachowań osoby fizycznej.

W.R.Wiewiórowski: *Nowe ramy ochrony danych osobowych w Unii Europejskiej*, Monitor Prawniczy - Dodatek 'Ochrona danych osobowych' [red:] G. Sibiga, Nr 7/2012, s. 1-8

Różne metody profilowania grupowego i indywidualnego opisuje M.Hildebrandt, *Defining Profiling: A New Type of Knowledge?* (w:) M.Hildebrandt, S.Gutwirth, *Profiling the European Citizen. Cross-Disciplinary Perspectives*, Springer 2008, s. 20-29. *Ibidem* kilka krytycznych uwag w: D.-O. Jaquet-Chiffelle: *Reply: Direct and Indirect Profiling in the Light of Virtual Persons*, s. 34-43.

M.Hildebrandt, *Who is Profiling Who ? Invisible Visibility* (w:) S.Gutwirth, Y.Poullet, P. de Hert, C. de Terwangne, S.Nouw, *Reinventing Data Protection ?*, Springer 2009, s. 241 oraz A.Canhoto, J.Blackmore, *General Description of the Process of Behavioural Profiling* (w:) M.Hildebrandt, S.Gutwirth: op.cit., s. 47-48.

KONTROWERSJE

Artykuł 20

Środki oparte na profilowaniu

1. Każda osoba fizyczna ma prawo nie podlegać środkowi, który wywołuje skutki prawne dotyczące tej osoby fizycznej lub ma istotny wpływ na tę osobę fizyczną, a który opiera się wyłącznie na automatycznym przetwarzaniu danych mającym służyć ocenie niektórych aspektów osobistych tej osoby fizycznej lub też analizie bądź przewidzeniu zwłaszcza wyników w pracy, sytuacji ekonomicznej, miejsca przebywania, zdrowia, preferencji osobistych, wiarygodności lub zachowania tej osoby fizycznej.

Z zastrzeżeniem innych przepisów niniejszego rozporządzenia, dana osoba może zostać poddana jednemu ze środków, o których mowa w ust. 1, jedynie wtedy gdy przetwarzanie: (...)

- b) jest wyraźnie dozwolone przez prawo Unii lub państwa członkowskiego, które ustanawia również właściwe środki w celu zabezpieczenia słusznych interesów podmiotu danych; lub
- c) odbywa się na podstawie zgody podmiotu danych, z zastrzeżeniem warunków określonych w art. 7 oraz właściwych gwarancji.

Automatyczne przetwarzanie danych osobowych, które ma służyć ocenie niektórych aspektów osobistych osoby fizycznej, nie opiera się jedynie na szczególnych kategoriach danych osobowych, o których mowa w art. 9. (...)

KONTROWERSJE

Artykuł 20 Środki oparte na profilowaniu

1. Każda osoba fizyczna ma prawo nie podlegać środkowi, który wywołuje skutki prawne dotyczące tej osoby fizycznej lub ma istotny wpływ na tę osobę fizyczną, a który opiera się wyłącznie na automatycznym przetwarzaniu danych mającym służyć ocenie niektórych aspektów osobistych tej osoby fizycznej lub też analizie bądź przewidzeniu zwłaszcza wyników w pracy, sytuacji ekonomicznej, miejsca przebywania, zdrowia, preferencji osobistych, wiarygodności lub zachowania tej osoby fizycznej.

2. Z zastrzeżeniem innych przepisów niniejszego rozporządzenia, dana osoba może zostać poddana jednemu ze środków, o których mowa w ust. 1, jedynie wtedy gdy przetwarzanie:

a) odbywa się w trakcie zawierania lub wykonania umowy, jeśli wniosek w sprawie zawarcia lub wykonania umowy złożony przez podmiot danych został

zrealizowany lub jeśli przewidziano właściwe środki w celu zabezpieczenia słuszných interesów podmiotu danych, jak np. prawo do uzyskania interwencji ze strony człowieka; lub

b) jest wyraźnie dozwolone przez prawo Unii lub państwa członkowskiego, które ustanawia również właściwe środki w celu zabezpieczenia słuszných interesów podmiotu danych; lub

c) odbywa się na podstawie zgody podmiotu danych, z zastrzeżeniem warunków określonych w art. 7 oraz właściwych gwarancji.

KONTROWERSJE

Artykuł 20 Środki oparte na profilowaniu

(...)

3. Automatyczne przetwarzanie danych osobowych, które ma służyć ocenie niektórych aspektów osobistych osoby fizycznej, nie opiera się jedynie na szczególnych kategoriach danych osobowych, o których mowa w art. 9.
4. W przypadkach o których mowa w ust. 2, informacje, które ma przekazać administrator na mocy art. 14, obejmują informacje dotyczące istnienia przetwarzania w drodze środka takiego jak ten, o którym mowa w ust. 1 oraz przewidywanego wpływu tego przetwarzania na podmiot danych.
5. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 86 w celu doprecyzowania kryteriów i warunków odpowiednich środków służących zabezpieczeniu słusznym interesów podmiotu danych, o których mowa w ust. 2.

KONTROWERSJE

- używanie tej metody ma trzy zasadnicze cele:

1. uzyskanie społecznej i psychologicznej oceny klienta
2. uzyskanie informacji o materialno - społecznym statusie klienta
3. opracowanie sugestii i strategii dla prowadzących działania marketingowe

Takie wyjaśnienie można by bez kłopotu zastosować do profilowania dla celów marketingowych, gdyby nie fakt, że

..... jest to teza z książki ekspertów FBI nt. profilowania zbrodniarzy, w której słowo „przestępca” zastąpiono słowem „klient”, a „śledztwo” „działaniami marketingowymi” 😊

Patrz: Holmes, R. M., & Holmes, S. T. : Profiling Violent Crimes: An Investigative Tool , Wyd. IV ,Thousand Oaks: Sage Publications, Inc. 2008

KONTROWERSJE

Rekomendacja CM/Rec (2010) 13 Komitetu Ministrów państw członkowskich Rady Europy

**w sprawie ochrony osób w związku
z automatycznym przetwarzaniem danych
osobowych podczas tworzenia profili**



*(Przyjęta przez Komitet Ministrów w dniu 23 listopada 2010 r.
podczas 1099. posiedzenia Wiceministrów)*

<https://wcd.coe.int/wcd/ViewDoc.jsp?id=1710949&Site=CM>

OFICJALNA I RZECZYWISTA AGENDA ZMIAN PRAWNYCH W UE – wg C.Bowdena

Review of Data Protection Directive

“official” agenda

- Principle of “Accountability”
- Right to be Forgotten
- *faux* “Privacy by Design”
- Privacy by Default (?)
- “flexible” export rules
- DPA forum shopping (aka “harmonization”)

the real privacy agenda

- “anonymisation”
- right to online access
- Privacy engineering
- Data minimization
- Art.29 fails to enforce against major Internet companies
- future of Safe Harbor ?
- DPA computer science competence ?

C.Bowden: *Privacy and Surveillance on Internet. What Happened and What Will Happen Next*, Panoptykon. Internet at the Crossroads, Warszawa 20 wrzesnia 2011 r.

DZIĘKUJĘ ZA UWAGĘ

IMPLEMENTACJA FATCA W ŚWIECIE PRZEPISÓW O OCHRONIE DANYCH OSOBOWYCH

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

Warszawa, 13 lutego 2013 r.

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

FATCA A RZECZNICY OCHRONY DANYCH OSOBOWYCH

- W związku z prośbą Komisji Europejskiej Grupa Robocza Art. 29 analizuje kwestię zgodności amerykańskiej *ustawy o ujawnianiu informacji finansowych o rachunkach zagranicznych na cele podatkowe* (dalej: FATCA) z dyrektywą 95/46/WE.
- Grupa Robocza Art. 29 analizuje dwa modele implementacji FATCA: pierwotny oraz zaproponowany przez UK, IT, ES, FR oraz DE w ich wspólnym oświadczeniu z 8 lutego 2012 r. (tzw: oświadczenie międzyrządowe).
- Uwagi GR29 przyjęły formę listu do DG ds. Podatkowych i Unii Celnej wysłanego w dniu 21 czerwca 2011 r. 1 sierpnia 2012 r.
- Dyrektor Generalny DG TAXUD odpowiedział na list GR29.
- 26 września 2012 r. Podgrupa ds. Finansowych przygotowała uwagi do odpowiedzi KE, wysłane 1 października. .

FATCA A RZECZNICY OCHRONY DANYCH OSOBOWYCH

- Na posiedzeniu Podgrupy w dniu 9 września 2012 r. ustalono, że Podgrupa nie będzie wnioskować o dalsze przedłużeniu mandatu do zajmowania się sprawą FATCA, po tym jak zostanie wysłany drugi list do KE. Jednak 29 listopada 2012 r. KE przysłała kolejny list, z pytaniem o alternatywny model przekazywania danych do USA, negocjowany przez Japonię oraz Szwajcarię. Brytyjski Rzecznik (ICO) dokonał częściowej analizy tego listu, natomiast pełna analiza ma być dopiero przygotowana (stan na 6 lutego 2013 r.). ICO proponuje także, aby Grupa Robocza Art. 29 udzieliła dalszego mandatu

FATCA

- **FATCA** – została uchwalona jako część *ustawy o bodźcach do zatrudniania w celu przywrócenia zatrudnienia (HIRE)*. Jest częścią *wewnętrznego kodeksu podatkowego* (części 1471-1474).
- Jej celem jest zapobieganie uchylaniu się od podatków obywateli USA korzystających z usług zagranicznych instytucji finansowych (FFI).
- Ustawa będzie miała zastosowanie także do tych klientów, którzy korzystali z tych instytucji przed datą jego wejścia w życie.
- Zgodnie z FATCA wszystkie FFI będą zobligowane do identyfikacji ich klientów.
- Co roku dane klientów w zakresie imienia, nazwiska, adresu, numeru identyfikacji podatkowej (TIN), bilansu na koncie (pod warunkiem, że przekracza on 1.000.000 \$), dochodów, wydatków oraz płatności będą przekazywane do urzędu podatkowego USA (IRS).
- W wyniku dyskusji, m.in. z Komisją Europejską, stwierdzono, że dane te mogą także być najpierw przekazywane do krajowych organów podatkowych a potem do IRS na podstawie umów bilateralnych, protokołów lub Memorandów o Porozumieniu (MoU), dołączonych do tych traktatów.

FATCA

- Początkowo planowano wymuszanie zgodności poprzez kary między innymi poprzez nakładanie na instytucje oraz na podatników, którzy nie wywiążą się z obowiązków 30% „podatek od wstrzymania”.
- Podobny podatek byłby nałożony na *passthru payments* przez FFI, działających zgodnie z FATCA na te FFI, które działają niezgodnie oraz osoby, które mają tam konta.
- W „międzyrządowym podejściu” przygotowanym 8 lutego stwierdzono, że FFI z tych państw nie podlegały by powyższymi karom, jednak brałyby one udział w zapewnianiu nakładania kar w przypadku *passthru payments* przekazywanych do FFI, które nie są zgodne z FATCA.
- Podejście międzyrządowe zredukowałoby bariery administracyjne poprzez usunięcie obowiązków: wchodzenia w umowy przez FFI z IRS, przekazywania informacji na temat kont amerykańskich bezpośrednio do IRS, zamykania kont osób, które niespełniają wymogów oraz wstrzymywania *passthru payments* do osób, które nie spełniają wymogów lub krajów partnerskich FATCA.

FATCA - ZGODNOŚĆ Z DYREKTYWĄ

- Grupa Robocza Art. 29 podkreśla, że dyrektywa 95/46/WE ma zastosowanie do każdej osoby fizycznej, którego dane są przetwarzane na terytorium UE, także obywateli amerykańskich
- **Niezbędność** – Przesyłanie zbiorów danych oraz ich przeszukiwanie a priori nie koniecznie jest najlepszą metodą osiągnięcia zgodności z zasadą niezbędności. Zamiast tego powinno się zastosować węższe, bardziej wyselekcjonowane środki oraz udowodnić ich niezbędność. GR29 szanuje prawo USA do zapewniania skuteczności swojego prawa podatkowego, jednak w przypadku braku podstawy prawnej nie widzi możliwości pogodzenia dyrektywy z FATCA.

FATCA - ZGODNOŚĆ Z DYREKTYWĄ

Proporcjonalność – aby zapewnić zgodność należy przeanalizować czy:

- a) przetwarzane dane osobowe są ograniczone do takiej ilości, która jest naprawdę konieczna do osiągnięcia celów FATCA.
- b) dane są przetwarzane tylko dla tych celów dla których zostały zebrane.
- c) nie można osiągnąć celów FATCA przetwarzając mniej danych osobowych to jest przez agregację, anonimizację, pseudo-anonimizację, etc.

Podstawa prawna – bez prawa krajowego państw UE, które rozciągnęłyby stosowność FATCA na ich terytorium, nie ma podstaw prawnych do przetwarzania danych. W przypadku gdyby je uchwalono wtedy państwa członkowskie mogłyby się powołać na art. 7 litera c) dyrektywy 95/46 (przetwarzanie danych jest konieczne dla ochrony żywotnych interesów osób, których dane dotyczą) lub 7 litera e) (przetwarzanie danych jest konieczne dla realizacji zadania wykonywanego w interesie publicznym lub dla wykonywania władzy publicznej przekazanej administratorowi danych lub osobie trzeciej, przed którą ujawnia się dane).

GR29 podkreśla, że zgoda nie może być podstawą z uwagi na nierównowagę pozycji osoby, której dane dotyczą oraz administratora danych oraz nieprawdopodobność możliwości odwołania zgody.

FATCA - ZGODNOŚĆ Z DYREKTYWĄ

Sprawowanie funkcji administratora danych na mocy FATCA – w przypadku przekazywania danych bezpośrednio przez FFI do IRS, FFI na pewno byłby administratorem.

W podejściu międzyrządowym krajowe instytucje podatkowe także określałyby przetwarzanie danych.

GR29 prosi KE oraz państwa członkowskie o doprecyzowanie roli instytucji podatkowych.

.

FATCA - ZGODNOŚĆ Z DYREKTYWĄ

Zgodność z zasadami ochrony danych – każdy administrator musi spełniać obowiązki wynikające z Art. 6 dyrektywy 95/46/WE. Szczególnie trzeba zwrócić uwagę na art. 6 punkt b) stanowiący, że *„dane osobowe były gromadzone do określonych, jednoznacznych i legalnych celów oraz nie były poddawane dalszemu przetwarzaniu w sposób niezgodny z tym celem.”*

Wszyscy administratorzy muszą jasno poinformować jak długo będą przechowywać oraz aktualizować dane. Trzeba się zastanowić jak osoba, której dane dotyczą może poinformować FFI, że jej dane, przekazane już do IRS, są niedokładne oraz zapewnić aby istniały mechanizmy pozwalające na poprawienie, usunięcie czy zablokowania danych.

Należy także zapewnić aby osoby, których dane dotyczą mogły wykorzystać prawa przysługujące im na mocy art. 11, 12 oraz 14 to jest przejrzystości, prawa dostępu, sprzeciwu, zablokowania oraz usunięcia danych.

Dane wrażliwe powinny być chronione w większym stopniu. Ponadto, administratorzy muszą zapewnić zgodność z art. 17 (bezpieczeństwo przetwarzania).

Powinno się poświęcić szczególną uwagę kwestii notyfikacji naruszeń ochrony danych pomiędzy administratorami. Należy także zapewnić istnienie że pracownicy mający dostęp do danych posiadają poświadczenie poufności.

Powyższa lista nie jest wyczerpująca.

FATCA - ZGODNOŚĆ Z DYREKTYWĄ

Przekazywanie do USA –IRS nie należy do programu Bezpiecznej Przystani. Tym samym:

- a) jeśli dane mogłyby być przekazywane przez FFI bezpośrednio wtedy należałoby spełnić warunki określone w art. 25 (przekazywanie danych osobowych do państw trzecich). Każde państwo musiałoby dokonać interpretacji tego artykułu co oznaczałoby m. in. uprzednią zgodę DPA, uprzednią notyfikację lub przeprowadzenie oceny zgodności na własną rękę. W przypadku podpisania umów dwustronnych należy zapewnić, że są one wiążące dla wszystkich stron.
- b) w przypadku zastosowania podejścia międzyrządowego ciężar zapewnienia zgodności z art. 25 oraz 25 (2) mógłby zostać przeniesiony lub współdzielony z instytucjami podatkowymi.
- c) w trzecim przypadku państwo nie korzysta z żadnej z powyższych dróg i wybiera podejście oparte na własnych przepisach.

GR29 podkreśla, że wyjątek z art. 26 ustęp 1 litera d) stanowiący, że można przekazać dane jeśli jest to *konieczne lub wymagane przez prawo z ważnych względów publicznych lub w celu ustanowienia, wykonania lub obrony tytułu prawnego* może zostać wykorzystany **tylko jeżeli istotny interes publiczny jest jasno zdefiniowany oraz wykazano, że przeważa on nad prawem do prywatności osoby**, której dane dotyczą.

FATCA - ZGODNOŚĆ Z DYREKTYWĄ

Dalsze przekazywanie – GR29 przypomina administratorom o konieczności zapewnienia przestrzegania obowiązków w zakresie dalszego przekazywania. Podejściu międzyrządowe może oznaczać stosowanie obecnych umów do przekazywania danych. Niektóre z nich obligują krajowe instytucje finansowe do zbierania i przekazywania danych do innego kraju nawet jeśli same nie mają podstawy prawnej do ich przetwarzania dla własnych celów. Umowy oferują pewne środki ochronne, nie wiadomo jednak czy umowy są wiążące w USA, dlatego należy zapewnić, że osoby, których dane dotyczą są w stanie wyegzekwować swoje prawa.

Nadzór oraz odwołania Choć w pierwszym rzędzie akt dotyczy obywateli USA, możliwe jest także przetwarzanie danych innych obywateli. GR29 nie jest pewna jak ich prawa będą chronione. Z tego względu GR29 uważa, że należy doprecyzować jak prawa tych osób będą chronione w zgodzie z dyrektywą. Prosi także ponownie KE przeanalizowanie możliwego uczestnictwa Komitetu Nadzorczego ds. Wolności Obywatelskich.

FATCA - ZGODNOŚĆ Z DYREKTYWĄ

PODSUMOWANIE – GR29 podziela obawy odnośnie jednoczesnego zapewnienie zgodności z Dyrektywą oraz FATCA. Podejście międzyrządowe pozwoliłoby na zastosowanie wiążących umów. GR29 podkreśla, że jedynie wiążąca umowa może być podstawą do przekazywania danych. Należy podkreślić, że podejście międzyrządowe jest jedynym rozwiązaniem i możliwe, że inne państwa będą musiały rozwinąć swoje podejścia jeżeli nie mogą go przyjąć. Ponadto biorąc pod uwagę niespójność, która może wynikać z wielości stanowisk być może należałoby przyjąć wspólne podejście na poziomie UE tak jak przy SWIFT czy PNR. GR29 podkreśla swoją gotowość do współpracy.

FATCA - STANOWISKO TAXUD

1. KE wypunktowała pewne nieścisłości dotyczące faktów jeśli chodzi o opinię GR29 na temat FATCA.
2. KE dopytała się, czy zdaniem GR29 środki ochronne zastosowane w Traktacie o Podwójnym Opodatkowaniu zawartym pomiędzy Stanami Zjednoczonymi a Zjednoczonym Królestwem są wystarczające dla przekazywania danych.
3. KE przedstawiła informację na temat alternatywnego podejścia, które jest negocjowane pomiędzy USA a Japonią oraz Szwajcarią. Ustanawia ono ramy pozwalające na bezpośrednie przekazywanie informacji przez FFI do IRS, przy czym wymagana jest zgoda właścicieli kont. Jednakże, jeśli nie udzielą oni zgody, wtedy państwa te godziłyby się na prośbę USA o przekazanie dodatkowych informacji na temat osób, które nie zgodziłyby się na przekazanie danych. Podstawą dla takiego przekazania informacji byłyby traktaty podatkowe pomiędzy USA a tymi państwami.

KE, zaznaczając, że rozumie, że zdaniem GR29 przekazanie danych osób bezpośrednio do IRS, za zgodą, byłoby niemożliwe z powodu braku równowagi pomiędzy stronami (osoby, których dane dotyczą z jednej strony i Stany Zjednoczone z drugiej), pyta się jednakże czy alternatywny model złamałby ramy ochrony danych w Unii Europejskiej.

FATCA - DODATKOWE STANOWISKO RZECZNIKÓW

1. Odnośnie nieścisłości, doceniając znaczenie dokładności informacji, GR29 stoi na stanowisku, że nie mają one zasadniczego znaczenia i nie zmieniają zarówno opinii GR29 jak i jej uwag.
2. Odnośnie tego, czy środki ochronne zastosowane w umowach podatkowych są wystarczające, GR29 wskazuje, że w swoim pierwszym liście napisała, że choć mogą one zaoferować pewne środki ochrony danych, to jednak państwa członkowskie oraz KE muszą zapewnić, że środki te są stosowane w praktyce. Oznacza to między innymi, że zasada ograniczenia celu jest przestrzegana oraz że istnieją środki ochronne łagodzące jej ewentualne złamanie oraz zapewniające istnienie środka odwoławczego. Istotne jest aby traktaty zapewniały odpowiedni poziom ochrony nawet wtedy gdy dane opuszczają już UE. Może to oznaczać, że należy znowelizować traktaty podatkowe.

GR29 podaje także dalsze przykłady środków ochronnych, których nie dostrzega w traktatach podatkowych oraz w modelu implementacji FATCA. Obejmują one następujące kwestie:

- a) w jaki sposób osoby, których dane dotyczą będą miały dostęp do danych, do kogo mają złożyć taki wniosek, jak długo będzie trwało jego rozpatrzenie oraz jakie bariery administracyjne będą musieli pokonać,
- b) w jaki sposób będzie zapewniony osobom, których dane dotyczą, środek odwoławczy; c) w jaki sposób umowy będą wiążące dla obu stron.

FATCA - ALTERNATYWNY MODEL PRZEKAZYWANIA DANYCH

KE, stwierdziła, że uwagi GR29 rozumie w ten sposób, że niektóre traktaty podatkowe będące obecnie w mocy mogą zawierać odpowiednie środki ochronne, podczas gdy inne ich nie posiadają.

KE wskazuje także, że niektóre państwa, które wyrażają obiekcje wobec automatycznego przekazywania danych mogą być zainteresowane wdrożeniem alternatywnego modelu (model 2), o ile ramy prawne UE w obszarze ochrony danych na to pozwolą. W dalszej części litu omówiono alternatywne klauzule. Poproszono także GR29 o opinię w tej kwestii.

FATCA - ALTERNATYWNY MODEL PRZEKAZYWANIA DANYCH

Alternatywny model klauzul (model II): W opinii KE jakkolwiek model II bazuje na modelu I, to jednak różni się od niego w trzech aspektach: mechanizmie informowania IRS; korzyściach dla FFI oraz odnośnie poziomu wzajemności zapewnianego przez USA.

- 1. Mechanizm dostarczanie informacji:** w przypadku modelu II przekazanie informacji będzie się odbywało po wyrażeniu zgody przez właściciela konta. Będzie on także poinformowany na piśmie o konsekwencjach braku wyrażenia takiej zgody. W przypadku wyrażenia takiej zgody FFI przekaże taką informację bezpośrednio do IRS. Jeżeli zgoda nie zostanie udzielona wtedy FFI będzie zobowiązana przysyłać co roku „zagregowane informacje” do IRS, dotyczące właścicieli kont. Wtedy IRS będzie mógł wystąpić z „grupową prośbą” o informacje na temat właścicieli kont do rządu państwa, w którym FFI ma siedzibę. Rządy mają 6 miesięcy na przekazanie tych informacji. Tak więc te same informacje i tak zostaną przekazane niezależnie od tego czy wyrażono zgodę. „Zagregowane raportowanie” będzie dotyczyło tylko istniejących kont (na dzień 31 grudnia 2013 r.), od 1 stycznia 2014 r. zgoda na przekazywanie takich informacji będzie konieczna do otwarcia konta.
- 2. Korzyści dla FFI** Korzyści dla FFI są uzależnione nie tylko od FFI ale także od rządów, ponieważ w dalszej procedurze to one mogą przekazać dane. Ponadto w modelu I FFI ma 18 miesięcy na naprawienie „istotnego” braku zgodności, podczas gdy w modelu 2 tylko 12 mies.
- 3. Wzajemność ze strony USA** Co do zasady w modelu 2 nie ma zasady wzajemności, ale partner może się zwrócić o taką informację do USA. Ponadto można także zawrzeć dodatkową umowę, która uwzględniałaby przestrzeganie takiej zasady.

FATCA - OPINIA BRYTYJSKIEGO RZECZNIKA INFORMACJI

Biuro GIODO zwróciło się także o opinię do Brytyjskiego Rzecznika Informacji (ICO) w kwestii FATCA.

Stwierdził on, że ICO zaakceptowało fakt, że Zjednoczone Królestwo przystało na kompromis polegający na zgodzeniu się na obowiązek prawny, nałożony na instytucje finansowe znajdujące się w jego jurysdykcji, przekazywania informacji podlegających FATCA brytyjskim organom podatkowym. Organy te będą używać istniejącego traktatu jako podstawy do dzielenia się tymi informacjami. ICO zwrócił także uwagę, że choć w dokumencie opublikowanym przez brytyjskie organy podatkowe zapisano: *„art. 7 ust. 3 (odnoszący się do Umowy Międzyrządowej) jasno stanowi, że HMRC jest zaangażowany w zapewnianie, że wymieniane informacje będą poddane odpowiednim środkom ochronnym, dotyczącym ich wykorzystania. Będzie to zapewnione poprzez zastosowanie istniejących zabezpieczeń oraz przepisów zawartych w naszych istniejących umowach o wymianie informacji”*, nie wiadomo istocie czym są te zabezpieczenia. ICO skontaktował się z organami podatkowymi w celu uzyskania dalszych wyjaśnień, ale powiedziano mu, że KE współpracuje ze wszystkimi państwami członkowskimi w celu zapewnienia odpowiednich środków ochronnych.

ICO stwierdza, że nie jest przekonany odnośnie zabezpieczeń danych, jako że nie ma dostępu do szczegółów tych zabezpieczeń. Na przykład, nie wiadomo jakie prawa przysługują osobom, których dane dotyczą, jeżeli ich dane były niedokładne powodując, że IRS ściga osobę, której dane dotyczą, domagając się pieniędzy na podstawie takich niedokładnych informacji – gdzie osoba, której dane dotyczą może złożyć sprzeciw, poprawić dane oraz odwołać się z powodu jakichkolwiek doznanych szkód lub stresu?

FATCA - DOTYCHCZASOWE DZIAŁANIA GIODO

KORESPONDENCJA Z MF:

GIODO skierował dwa pisma do Ministra Finansów (24 lutego 2012 r. i 20 czerwca 2012 r.) z pytaniem o FATCA.

MF odpowiedział w dniu 11 lipca 2012 r. wskazując, że brak opinii GR29 jest jednym z czynników opóźniających podjęcie decyzji odnośnie zakresu prac nad prawem wdrażającym FATCA.

Napisano, że po konsultacjach z Departamentem Skarbu, Polska skłania się ku opcji „*government to government*” zbliżonej do tej ze wspólnego oświadczenia USA, FR, DE, UK, ES i IT. Ostateczna decyzja miała być podjęta po przedstawieniu wzoru umów przez USA.

W piśmie z dnia 31 lipca 2012 r., GIODO podziękował MF za informację i poprosił o dalsze informowanie w tej sprawie. Następnie w dniu 3 września 2012 r.

.

FATCA - DOTYCHCZASOWE DZIAŁANIA GIODO

KORESPONDENCJA ZE ZWIĄZKIEM BANKÓW POLSKICH:

GIODO wysłał pismo w dniu 12 stycznia 2012 r. (w odpowiedzi na pismo Banków) do Pana Jerzego Bańki, Wiceprezesa Związku Banków Polskich

Odnosząc się do kwestii nakładania przez FATCA obowiązków na polskie instytucje GIODO wymienił źródła powszechnie obowiązującego prawa w Polsce. Ponadto stwierdził, że akt prawny obowiązujący w innym kraju niż Polska, nie może nakładać obowiązków na osoby fizyczne ani prawne w Polsce. Ponadto, biorąc pod uwagę, że USA są państwem trzecim i nie zapewniają odpowiedniego poziomu ochrony danych, ewentualne umowy musiałyby zawierać odpowiednie środki ochronne. GIODO poinformował także, że nie są mu znane żadne ustalenia w tej kwestii oraz że jest gotowy do współpracy.

DZIĘKUJĘ ZA UWAGĘ