Informacja o pracach nad reformą unijnego prawa dot. ochrony prywatności i danych osobowych
zasady konsultacji w ramach sektora ubezpieczeniowego, kierunki zmian, ich skutki dla ZU

XI edycja
Seminarium Polskiej Izby Ubezpieczeń

dr Stefan Szyszko
Dyrektor Działu Zarządzania Informacją Ubezpieczeniową
Polska Izba Ubezpieczeń

Warszawa, 19 kwietnia 2012 r.

Agenda

- Przyczyny reformy KE prawa o ochronie danych osobowych w UE
- Kierunki prac KE
- Harmonogram prac KE
- Forum konsultacyjne
- Branża ubezpieczeniowa a reforma wdrażana przez KE
- Skutki reformy dla prawa krajowego
- Szczegółowe omówienie projektu Rozporządzenia
- Dane źródłowe

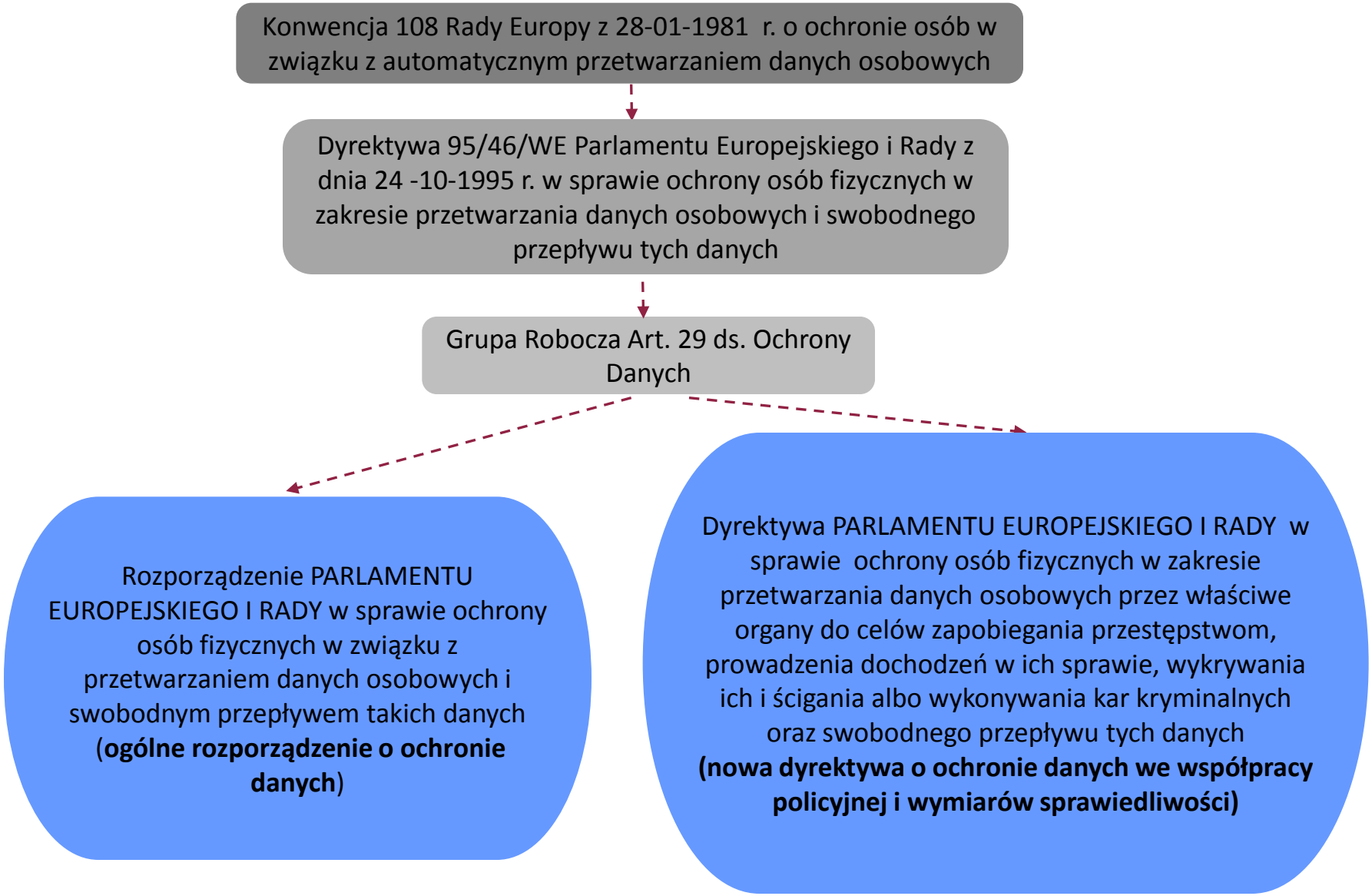
Ochrona danych osobowych – prawo wspólnotowe

- **Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych.**
- **Dyrektywa 97/66/WE Parlamentu Europejskiego i Rady z dnia 15 grudnia 1997 r. w sprawie przetwarzania danych osobowych i ochrony prywatności w dziedzinie telekomunikacji.**
- **Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady WE z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług w społeczeństwie informacyjnym, a w szczególności handlu elektronicznego w obrębie wolnego rynku.**
- **Dyrektywa Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. 2002/58/WE w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze komunikacji elektronicznej (Dyrektywa o ochronie prywatności i komunikacji elektronicznej).**
- **Dyrektywa Parlamentu Europejskiego i Rady WE z dnia 15 marca 2006 r. 2006/24/WE w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE.**

Przyczyny reformy KE prawa o ochronie danych osobowych w UE

- **Zakończenie „okresu refleksji” po gruntownym przeglądzie sytuacji w ochrony danych w EOG przez tzw. Grupę Roboczą Art. 29 (2009-11)**
- **Reakcja na oddziaływanie nowych technologii: umasowienie przetwarzania danych oraz zmiany społeczne i gospodarcze stąd wynikające :**
  - **Obecna „muzealna” Dyrektywa jest z epoki „przed-internetowej” – 1995 r. !!!**
  - W całych obszarach budzi zasadnicze wątpliwości interpretacyjne (przetwarzanie mobilne, cloud computing)
  - Coraz bardziej zagrożona jest ochrona prywatności, stąd pomysły na polepszenie jej skuteczności w sposób nieszkodliwy z gospodarczego punktu widzenia
- **Reakcja na globalizację oraz umasowienie międzynarodowego przekazywania danych:**
  - Obiektywna potrzeba zwiększenia faktycznych gwarancji ochrony prywatności
  - Uznanie konieczności większego oparcia się na samoregulacji (dobre praktyki, etc.)
- **Zwiększenie spójności ram prawnych w zakresie ochrony danych w ramach jednolitego rynku europejskiego:**
  - Eliminacja niespójności interpretacyjnych w krajach EOG, hamujących rozwój gospodarki elektronicznej
  - Krajowe różnice są hamulcem rozwoju nowoczesnej gospodarki, obniżają globalną konkurencyjność UE
  - Inicjatywa intensywnie wspierana przez Viviane Reding, Komisarz ds. sprawiedliwości, wymiaru sprawiedliwości i obywatelstwa w KE
- **Ujednolicenie norm prawnych przetwarzania danych osobowych wrażliwych:**
  - Ambicja połączenia lepszych gwarancji ochrony praw podmiotów danych z minimalizacją utrudnień o charakterze ekonomicznym i prawnym wskutek rozbieżności definicji danych osobowych „wrażliwych” w państwach członkowskich (np. dane biometryczne)

Kierunki prac KE



Kierunki prac KE – akty do zmiany oraz proponowane sposoby jej wprowadzenia

PRAWO WSPÓLNOTOWE

- **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**
  - **Rozporządzenie PARLAMENTU EUROPEJSKIEGO I RADY w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych)**
  - Nowa Dyrektywa PARLAMENTU EUROPEJSKIEGO I RADY w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz swobodnego przepływu tych danych:
    - Jako uzupełnienie normy ogólnej – ze względu na wagę przetwarzania danych przez organa oraz szereg wyłączeń, skutkujących dużymi różnicami w EOG
    - Dyrektywa a nie Rozporządzenie – ze względu na skalę różnic krajowych

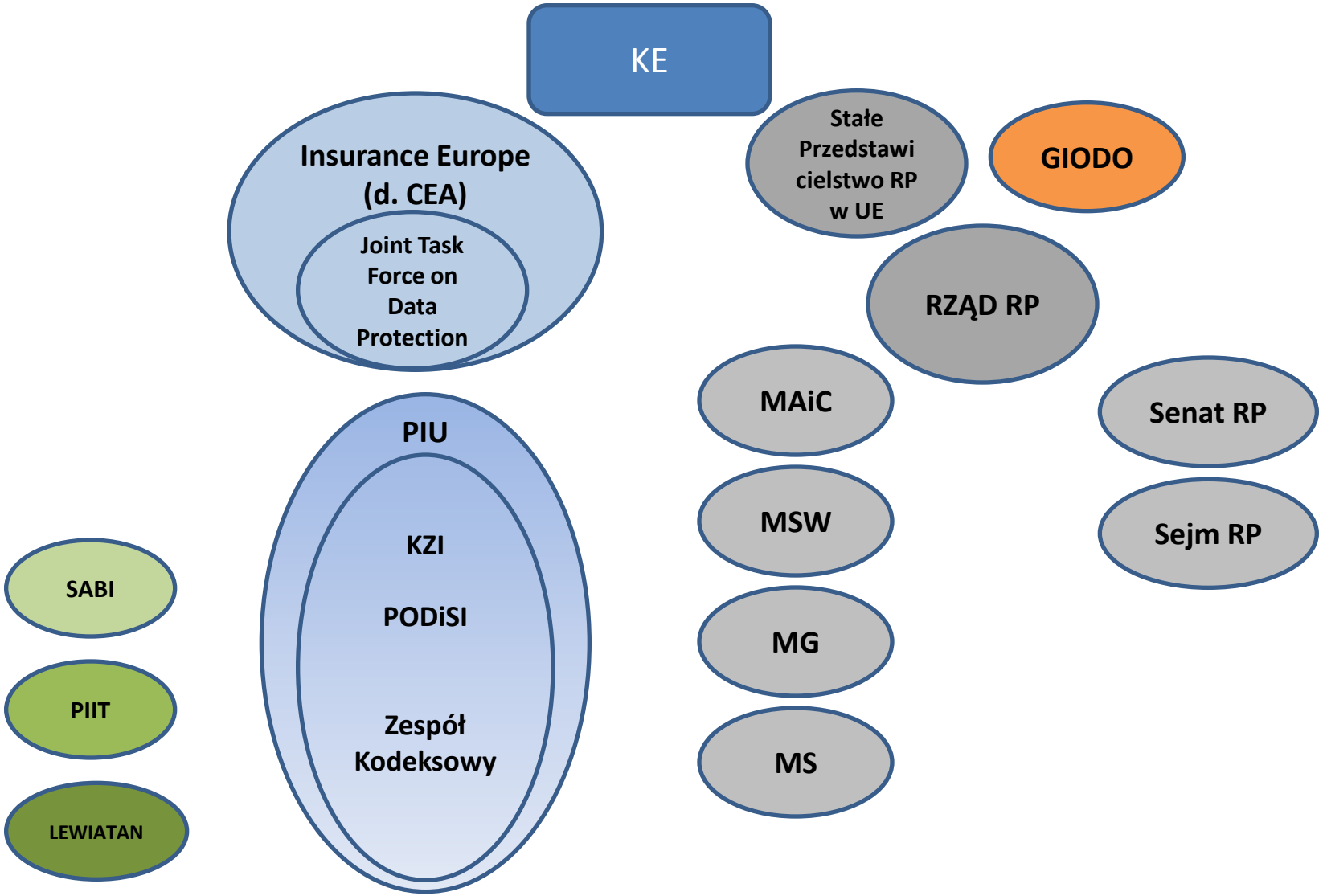
PRAWO MIĘDZYNARODOWE

- **Konwencja 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (sporządzona w Strasburgu dnia 28 stycznia 1981 r.)**
- Aktualizacja Konwencji, w sposób zsynchronizowany z 2 w/w propozycjami

Projektowany harmonogram prac KE nad reformą prawa ochrony danych

maj-grudzień 2009	4 listopada 2010	6 grudnia 2011	25 stycznia 2012	2013	2014	2015
KE zainicjowała przegląd ram prawnych, rozpoczynając od konferencji na wysokim szczeblu w maju 2009 r., po której nastąpiły konsultacje publiczne prowadzone do końca 2009 r.	KE przyjęła Komunikat Strategiczny o zamiarze "Kompleksowego podejścia do ochrony danych osobowych w UE" i rozpoczęła publiczne konsultacje. CEA wniosła do nich wkład na szczeblu Komisji Europejskiej, bazujący również na konsultacjach poczynionych przez PIU na polskim rynku ubezpieczeniowym	Wiceprzewodnicząca Komisji Europejskiej Viviane Reding - Komisarz ds. Wymiaru Sprawiedliwości i Obywatelstwa zapowiedziała, że na proponowane nowe ramy prawne składają się dwa wnioski legislacyjne: - ogólne rozporządzenie o ochronie danych - Nowa Dyrektywa o ochronie danych we współpracy policyjnej i wymiarów sprawiedliwości	Wiceprzewodnicząca Komisji Europejskiej - Viviane Reding, Komisarz ds. Wymiaru Sprawiedliwości i Obywatelstwa, zaprezentowała oficjalnie projekt zmiany unijnych przepisów dotyczących ochrony danych osobowych	Konsultacje w ramach UE: PROCES BARDZO CZASO- I PRACOCHŁONNY		Planowane wdrożenie

Forum konsultacyjne



Percepcja europejska projektowanych zmian – BARDZO ZRÓŻNICOWANA

- **Rozporządzenie PARLAMENTU EUROPEJSKIEGO I RADY w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych)**
  - Wątpliwości co do zgodności z zasadą pomocniczości, SZCZEGÓLNIE WSKUTEK BARDZO DUŻEJ LICZBY AKTÓW DELEGOWANYCH
  - Zasadnicze wątpliwości, czy w prawie krajowym można ustanowić zasady bardziej restrykcyjne
  - Skrajnie różne opinie w kwestiach ABI:
    - Niemcy: postulowane wzmocnienie, wdrożone w reformie prawa krajowego
    - Czechy, W. Brytania: całkowity brak ABI dotąd i pogląd że jest to funkcja zbędna
- **Dyrektywa PARLAMENTU EUROPEJSKIEGO I RADY w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz swobodnego przepływu tych danych**
- Analogiczne obawy o zgodność z zasadą pomocniczości
- Zdecydowanie większy opór niż w przypadku Rozporządzenia, ponieważ:
  - Nowa Dyrektywa nakazuje podporządkowanie wszystkich nowych o już zawartych umów międzynarodowych nowym zasadom
  - Wbrew tytułowi, Dyrektywa nie ogranicza się do regulowania wymiany międzynarodowej danych, lecz ustanawia nowe standardy w prawie krajowym
  - To z kolei budzi sprzeczne opinie: dla jednych krajów jest to wzmocnienie, a dla innych osłabienie istniejących zasad ochrony danych
- **ELEMENT WSPÓLNY: DUŻE KOSZTY WDROŻENIA ZMIAN**

Forum konsultacyjne – obiegi informacji

- **Krajowy**
  - Sejm RP - Komisja ds. Unii Europejskiej – koordynuje sprawy związane z członkostwem RP w UE, m.in. zajmuje stanowisko i wyraża opinii na temat projektów aktów prawnych UE, formułowanie zaleceń dla Rady Ministrów dotyczących stanowiska RP, jakie RM ma zamiar zająć podczas rozpatrywania projektu w Radzie
  - Rząd RP:
    - Ministerstwo Administracji i Cyfryzacji – Podsekretarz Stanu, Igor Ostrowski – przedstawiciel Rządu RP upoważniony do prezentowania stanowiska Rządu w sprawie projektu Rozporządzenia.
    - Ministerstwo Spraw Wewnętrznych – Sekretarz Stanu, Piotr Stachańczyk – przedstawiciel Rządu RP upoważniony do prezentowania stanowiska Rządu w sprawie projektu nowej Dyrektywy o ochronie danych we współpracy policyjnej i wymiarów sprawiedliwości.
- **Unijny ubezpieczeniowy**
  - Europejski Komitet Ubezpieczeń - Insurance Europe (d. CEA)
  - W nim Joint Task Force on Data Protection
- **Wehikuł Izbowy konsultacji z ZU:**
  - Legislacje
    - Legislacji PIU nr 13/2011 (15-02-2011)
    - Legislacji PIU nr 111/2011 (21-12-2011)
    - Legislacji PIU nr 9/2012 (3-02-2012)
    - Legislacji PIU nr 34/2012 (4-04-2012)
  - Komisje, Podkomisje, Zespoły Robocze
    - Komisja Zarządzania Informacją Ubezpieczeniową PIU
    - Podkomisja Ochrony Danych i Standaryzacji Informacji
    - Zespół Roboczy przy PODiSI ds. Wypracowania Kodeksu Dobrych Praktyk Ochrony Danych Osobowych w Ubezpieczeniach

Branża ubezpieczeniowa a reforma prawa unijnego

- **Co w tych projektach dotyczy ZU i dlaczego**
  - Rozporządzenie PARLAMENTU EUROPEJSKIEGO I RADY w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych):
  - Nowa krajowa ustawa o ochronie danych osobowych - w zakresie nieuregulowanym nowym Rozporządzeniem PEiR oraz aktami wykonawczymi do niego
- **Skutki dla ZU:**
  - wzrost obowiązków i kosztów po stronie zakładów (m.in. nowy obowiązek 24-godzinnego powiadamiania podmiotu danych oraz organu nadzoru o każdym istotnym naruszeniu ochrony danych osobowych, przeprowadzanie dodatkowej analizy ryzyka tzw. „oceny wpływu ochrony danych”)
  - Zwiększenie zasobów dla realizacji rozszerzonego zakresu zadań Administratora Bezpieczeństwa Informacji
  - Koszty adaptacji i utrzymania systemów informatycznych (m.in. wprowadzenie „prawa do bycia zapomnianym” tzn. usuwania zbędnych danych ze zbiorów danych, „prawo do wycofania zgody na przetwarzanie danych”)
  - Zaostrzenie kryteriów adekwatności danych do celów ich przetwarzania (postulat minimalizacji zakresu danych co stoi w sprzeczności z potrzebami wielu procesów ubezpieczeniowych: ocena ryzyka ubezpieczeniowego w procesach akwizycji i obsługi świadczeń)
  - Wzrost obciążeń biurokratycznych i ryzyka reputacyjnego

Skutki dla prawa krajowego reformy KE

- **Zapewne konieczne będą zmiany w krajowych aktach prawnych m.in. Ustawy o ochronie danych osobowych, ustawy o świadczeniu usług droga elektroniczną, prawo telekomunikacyjne, etc.**
- **Najprawdopodobniej zbędne będzie krajowe rozporządzenie do ustawy o ochronie danych osobowych:**
  - Obecne jest muzealne
- **W projekcie rozporządzenia Unijnego pojawiają się:**
  - Nawiązania do norm technicznych z obszaru bezpieczeństwa informacji
  - Wzmocnienie roli samoregulacji

Szczegółowe omówienie projektu Rozporządzenia

- **Rozdział I przepisy ogólne**
  - Uzupełnienie o zakres materialny i terytorialny rozporządzenia (art. 2 i 3)
  - Nowa definicja terminów „naruszenie ochrony danych osobowych”, „dane genetyczne”, „dane biometryczne”, „dane dotyczące zdrowia”, „główna siedziba”, „przedstawiciel”, „przedsiębiorstwo”, „grupa przedsiębiorców”, „wiążące reguły korporacyjne”, „definicja dziecka”, „organ nadzorczy” (art. 4)
- **Rozdział II zasady**
  - Określenie zasad przejrzystości, wyjaśnienie zasad minimalizacji danych, ustalenie zasad ponoszenia całkowitej odpowiedzialności przez administratora (art. 5)
  - Dookreślenie kryterium równowagi interesów (art. 6)
  - Uszczegółowienie warunków, które muszą zostać spełnione, by zgoda stanowiła ważną podstawę prawną (art. 7)
  - Przetwarzanie danych osobowych dzieci w odniesieniu do oferowanych im bezpośrednio usług społeczeństwa informacyjnego (art. 8)
  - Ogólny zakaz przetwarzania danych wrażliwych i szczególne odstępstwa od tego zakazu (art. 9)
- **Rozdział III prawa podmiotu danych**
  - Przejrzystość i tryby wykonywania praw w tym obowiązek informacyjny, dostęp do danych i ich poprawianie i usuwanie, prawo wniesienia sprzeciwu i profilowania (sekcja 1, 2, 3,4)

Szczegółowe omówienie projektu Rozporządzenia

- **Rozdział IV administrator i podmiot przetwarzający**
  - Uwzględnienie tematu „zasady odpowiedzialności” administratorów i ich współpracy z organem nadzorczym , w tym uszczegółowienie zasad zabezpieczenia danych oraz obowiązek zawiadamiania o naruszeniu ochrony danych, przeprowadzanie „analizy ryzyka danych osobowych”, **nowe obowiązki Administratora Bezpieczeństwa Informacji** (sekcja 1, 2, 3, 4)
- **Rozdział V przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych**
  - Uprawnienia KE do decydowania o odpowiednim poziomie ochrony zapewnianego na terytorium państwa trzeciego oraz mechanizmy współpracy międzynarodowej na rzecz ochrony danych między KE a organami nadzorczymi państw trzecich (art. 41-45)
- **Rozdział VI niezależne organy nadzorcze**
  - Określenie obowiązków i uprawnień oraz rozszerzenie wzajemnej współpracy między organami nadzorczymi z KE (Sekcja 1, 2)
- **Rozdział VII współpraca i zgodność**
  - Klarowność i ujednolicenie przepisów o wzajemnej pomocy, wspólnych operacji przeprowadzanych przez organy nadzorcze a także ustanowienie niezależnej Europejskiej Rady Ochrony Danych, w skład której wchodzą szefowie organów (Sekcja 1, 2, 3)

Szczegółowe omówienie projektu Rozporządzenia

- **Rozdział VIII środki ochrony prawnej, odpowiedzialność i sankcje**
  - Prawo osoby do złożenia skargi do organu nadzorczego oraz wprowadzenia tzw. pozwów zbiorowych oraz sądowych środków ochrony prawnej przeciwko organowi nadzorczemu/administratorowi/podmiotowi przetwarzającemu, w wyniku tego wprowadzenie prawa do odszkodowania oraz zobowiązania państw członkowskich do ustanowienia przepisów dotyczących kar i ich nakładania za naruszenie rozporządzenia (art. 73-79)
- **Rozdział IX przepisy dotyczące szczególnych sytuacji przetwarzania danych**
  - Stosowanie wyłączeń i odstępstw od przepisów rozporządzenia a prawo wolności wypowiedzi , uszczegółowienie kategorii danych przetwarzanych na potrzeby świadczenia opieki zdrowotnej oraz w kontekście zatrudnienia i statystyki oraz badań naukowych (art. 80-85)
- **Rozdział X akty delegowane i akty wykonawcze**
  - Uregulowanie szczegółowe rozwiązań z rozporządzenia w aktach wykonawczych (art. 86, 87).

Dokumenty źródłowe - resume

- **Konwencja 108**
  http://prawo.money.pl/akty-prawne/ujednolicone-akty-prawne/kodeksy/konwencja;nr;108;rady;europy;o;ochronie;osob;w,2003,3,25,DU,1155.html

- **Komunikat KE z dn. 4-11-2010 pt.„Całościowe podejście do kwestii ochrony danych osobowych w UE”** http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_pl.pdf

- **Dyrektywa (95)**
  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:pl:NOT

- **Projekt ogólnego rozporządzenia o ochronie danych z 25-01-2012**
  http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_pl.pdf

- **Projekt Dyrektywy „policyjnej” z dn. 25-01-2012**
  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012PC0010:en:NOT

Polska Izba Ubezpieczeń

Dziękuję za uwagę

Pytania i odpowiedzi