寧為太平犬，不做亂世人

Obyś żył w ciekawych czasach

Polska i europejska ochrona danych osobowych – remont czy przebudowa?

Jarosław Żabówka
proinfosec@odoradca.pl

Zawartość prezentacji

- Geneza i budowa prawa ochrony danych osobowych
- Planowana nowelizacja Konwencji
- Planowane zmiany w polskim prawie
- Rozporządzenie UE

Geneza i budowa prawa ochrony danych osobowych

- Prywatność a ochrona danych osobowych. Europejska Konwencja Praw Człowieka z 1950r.
- Lata 50 –pierwsze akty prawne, ustawa o ochronie danych osobowych w Hesji w 1970r, w kolejnych latach ustawy w poszczególnych krajach UE, 1973, 1974 – Rezolucje (rekomendacje) Rady Europy
- Rekomendacja Organizacji Współpracy Gospodarczej i Rozwoju (OECD) z dnia 23 września 1980 r. w sprawie wytycznych dotyczących ochrony prywatności i przekazywania danych osobowych pomiędzy krajami
- Konwencja Rady Europy Nr 108 z dnia 28 stycznia 1981 r. o Ochronie Osób w Związku z Automatycznym Przetwarzaniem Danych Osobowych – pierwszy poważny akt międzynarodowy, wszedł w życie 1.10.1985r, w Polsce 24.04.2002r.

Geneza i budowa prawa ochrony danych osobowych

- 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 w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze komunikacji elektronicznej, …
- Art. 47 Konstytucji RP: „*Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.*”

Inne koncepcje

- Warto zauważyć, że poza UE i USA obowiązują również inne systemy ochrony danych osobowych. Moim zdaniem warto zauważyć rozwiązania w:
- Kanadzie – „privacy by design”
- Australii – „privacy impact assessment”

Jakich zmian możemy się spodziewać w UE

- Konwencja
- Rozporządzenie i Dyrektywa

Planowane zmiany w Konwencji

Planowana jest nowelizacja Konwencji Rady Europy Nr 108 z dnia 28 stycznia 1981 r. o Ochronie Osób w Związku z Automatycznym Przetwarzaniem Danych Osobowych

- Uszczegółowienie zapisów Konwencji
- Zapewnienie zgodności i spójności z ramami prawnymi UE
- Utrzymanie neutralności technologicznej przepisów
- Utrzymanie uniwersalnego standardu Konwencji i jej otwartego charakteru

Planowane zmiany w Konwencji – wybrane zmiany

- Celem Konwencji staje się również zapewnienie wolności wypowiedzi i wolności do informacji. Z drugiej jednak strony, podkreśla się, że Konwencja dotyczy bezpieczeństwa informacji. Podkreśla się prawo osób do decydowania o swoich własnych danych
- Konwencja będzie dotyczyć „jurysdykcji” a nie „terytorium” UE
- Konwencja nie będzie dotyczyć danych przetwarzanych w celach domowych, ale musi uwzględniać sieci społecznościowe.
- Jednoznacznie stwierdza się, że Konwencja dotyczy również danych nie przetwarzanych automatycznie.

Planowane zmiany w Konwencji – wybrane zmiany

- „Automated data file” zastępujemy „structured files”
- „Automatic processing” staje się „data processing”
- Doprecyzowuje się definicję danych osobowych – zgodnie z Dyrektywą oraz szereg innych pojęć –„controller”, „data processing”, „file”. Wprowadza się: „recipient”, „processor”.
- Porządkuje się „przetwarzanie” – teraz obejmuje również zbieranie i przechowywanie.
- Dane wrażliwe – doprecyzowujemy i jednoznacznie nie robimy różnicy między przetwarzaniem automatycznym a zwykłym.
- Zabezpieczamy dane przed utratą a nie tylko przed przypadkową utratą.
- Procesora wybieramy w taki sposób, żeby zapewniał właściwe bezpieczeństwo danych.

Planowane zmiany w Konwencji – wybrane zmiany

- Musi być zapewniona „przejrzystość” przetwarzania danych obejmująca informowanie o administratorze, celu przetwarzania, odbiorcach, itd. (np. przekazywaniu do państwa trzeciego).
- Przetwarzanie danych musi być proporcjonalne do interesów, praw i wolności osób, których dane są przetwarzane oraz użyte środki i metody muszą być jak najmniej wpływać na naruszenie tych interesów, praw i wolności.
- Osoba musi otrzymać informacje o źródle danych.
- Dodaje się obowiązek zapewnienia w prawie stosowania adekwatnych zabezpieczeń (np. jako zadanie ABI).
- Rozszerza się zapisy o transgranicznym przesyłaniu danych.
- …

Jakich zmian możemy się spodziewać w Polsce

- Nowe rozporządzenie wykonawcze do uodo (być może również nowelizacja ustawy).
- Nowelizacja ustawy o świadczeniu usług drogą elektroniczną.
- Nowelizacja rozporządzenia o krajowych ramach interoperacyjności

Zmiany dla administracji publicznej

- Rozporządzenie o krajowych ramach interoperacyjności mówi jak powinny być budowane systemy teleinformatyczne w administracji.
- W projekcie rozporządzenia powołano normy, m.in. PN-ISO/IEC 20000, PN-ISO/IEC 27001, PN-ISO/IEC 17799, PN-ISO/IEC 27005, PN-ISO/IEC 24762
- Wydaje się, że z rozporządzenia nie wynika obowiązek stosowania tych norm – ale rozporządzenie mówi, że jeżeli będą one stosowane, to jego wymogi będą spełnione.

Ustawa o świadczeniu usług drogą elektroniczną

- Usunięcie art. 16 i 17 – stosować się będzie uodo.
- Nie musimy informować o procesorach.
- Rozszerzono obowiązek informacyjny.
- Uchyla się zakaz zestawiania danych usługobiorcy z jego pseudonimem (bo nie było to stosowane…).
- Nie zgodzono się z opinią GIODO, że ustawa powinna obejmować również przetwarzanie danych w celach prywatnych.
- Blokowanie dostępu do danych osób trzecich.
- …

Rozporządzenie UE

- Jednolite, ogólnoeuropejskie prawo
- Wprowadza definicje pojęć do tej pory niejasnych
- Wprowadza obowiązek informowania o naruszeniach
- Obowiązek prowadzenia analizy wpływu
- Prawo do bycia zapomnianym
- Określa rolę ABI

Rozporządzenie UE - zmiany

- W policji i sądownictwie będzie obowiązywać dyrektywa.
- Zmiana pozycji i zakresu zadań ABI. O tym rozmawialiśmy na poprzednim Spotkaniu, zapraszam do prezentacji i tekstu na stronie.
- Nieco rozszerzamy definicję danych osobowych. Obecnie są to dane które pozwalają na zidentyfikowanie osoby przez ADO lub „any natural or legal person”.
- Pojawiają się definicje "personal data breach", "biometric data", "data concerning health", "genetic data", "main establishment", "child".
- Adres, Adres IP, cookie – stają się jednoznacznie danymi osobowymi.
- Dane sensytywne zostają rozszerzone o genotyp i dane biometryczne.
- Regulacja obejmuje pozaeuropejskie przedsiębiorstwa przetwarzające dane lub monitorujące mieszkańców UE, jeżeli to działania jest skierowane do mieszkańców UE (prowadzone w lokalnym języku, w serwisie w narodowej domenie) – w miejsce obecnego przetwarzania na sprzęcie znajdującym się na terenie UE.
- W wypadku prowadzenia działalności na terenie większej ilości państw członkowskich, ADO będzie podlegał odpowiednikowi GIODO, na terenie którego ma siedzibę.

Rozporządzenie UE - zmiany

- Grupa robocza Art. 29 staje się – „European Data Protection Board”
- Projekt zawiera osobny rozdział na temat zgody na przetwarzanie danych. Jest to „dobrowolne, wyraźne i świadome wyrażenie woli”. Zwraca się uwagę, że zgodna nie będzie ważna, jeżeli występuje nierównowaga w zależności osoby od administratora. Zgoda dziecka będzie obowiązywać jedynie w wypadku jej autoryzowania przez rodzica. Zgoda będzie nieważna, jeżeli nie może być wycofana bez indywidualnej szkody. Generalnie stosowanie zgody, jako przesłanki legalizującej przetwarzanie danych jest odradzane.
- Nowe prawo - “right to be forgotten and erasure”.
- “Impact assessments” – nowy obowiązek dla ADO

Rozporządzenie UE - zmiany

- “Prior authorization/consultation” – czyli wymagana zgoda GIODO, w wypadku przetwarzania w wyższym stopiu zagrażającym prywatności.
- Dane dotyczące skazań powinny być przetwarzane jedynie pod kontrolą władzy publicznej.
- Obowiązek informowania osoby i organu nadzoru w wypadku naruszenia bezpieczeństwa.
- Obowiązek uzyskania zgody na transfer danych do państwa trzeciego, zagrożony wysoką odpowiedzialnością finansową. Ograniczenia w dostępnie do danych, dla organów sądowych państw trzecich.

Rozporządzenie UE - kontrowersje

- Bardzo wysokie kary.
- Projekt jest bardzo ambitny, ale prawdopodobnie będzie podlegał zmianom.
- Już odezwały się głosy sprzeciwu, np. z USA
- Główna krytyka dotyczy – kar, wymiany danych z państwami trzecimi, prawa do bycia zapomnianym

Bardzo dziękujemy za uwagę i zapraszamy do dyskusji.

感謝您的關注！