# SPOTKANIE INFORMACYJNE

**Zapewnij bezpieczeństwo informacji stosując międzynarodowe standardy wynikające z norm ISO 27001**

**16 czerwca 2016**
**Warszawa Centrum Szkoleniowo-Konferencyjne JUPITER**

**Prelekcja:** **Wybrane aspekty bezpieczeństwa informacji – ochrona danych osobowych”**

**Prelegent:** **Robert Radko**

**Agenda:**

**Zmiany w prawie ochrony danych osobowych wprowadzone tzw. „Ustawą 500+”**

**Wybrane zmiany i Nowości wprowadzone przez RODO czyli „Jak przygotować się do zmian w przepisach prawa ochrony danych osobowych w zawiązku z wejściem w życie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)”**

# Jakie zmiany UODO w związku z nowelizacją 500+ ?

- Zmienia się podejście do definicji Administratora danych osobowych
- Wyłącza się obowiązek umownego powierzania zbiorów danych osobowych pomiędzy podmiotami administracji publicznej

# ADO w kontekście 500+ (przyczyna zmian)

**Pismo Minister Rodziny, Pracy i Polityki Społecznej zgłaszające uwagi do projektu tzw. „ustawy 500+” FS4.021.48.2015/3a.856.CWS.15**

II. Ponadto proponuję w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2014 r. poz. 1182 ze zm.) wprowadzić następujące zmiany:

- w art. 23 po ust. 2 dodaje się ust. 2a w następującym brzmieniu:
  „2a. Podmioty, o których mowa w art. 3 ust. 1, uważa się za jednego administratora danych, jeżeli przetwarzanie danych służy temu samemu interesowi publicznemu.”
- w art. 31 po ust. 2 dodaje się ust. 2a w następującym brzmieniu:
  „ust. 2a. Nie wymaga zawarcia umowy między administratorem a podmiotem, o którym mowa w ust. 1, powierzenie przetwarzania danych, w tym przekazywanie danych, jeżeli ma miejsce między podmiotami, o których mowa w art. 3 ust. 1.”

Nowa regulacja wprowadza kolejne świadczenie oparte o powielany model świadczeń rodzinnych i społecznych. Wiele spośród dotychczas istniejących w systemie polityki rodzinnej i społecznej usług przenika się. Wiele wypłacanych świadczeń jest wzajemnie powiązanych (np. kryteria dochodowe, czy wymagany określony status beneficjenta świadczeń). Aktualnie obowiązujące uregulowania prawne w dużej mierze ograniczają możliwości wymiany danych między instytucjami obszaru rynku pracy i polityki społecznej – głównie z uwagi na ochronę danych osobowych i brak odpowiednich

# ADO w kontekście 500+ (przyczyna zmian)

uregulowań (lub niekorzystną interpretację istniejących) w ustawach szczegółowych. Mamy do czynienia z różnymi bazami danych, posiadającymi różnych Administratorów Danych Osobowych – co stanowi dużą przeszkodę w integracji informacji o kliencie korzystającym z różnych usług rynku pracy i polityki społecznej.

Instytucje realizujące różne programy tylko w ograniczonym zakresie wymieniają między sobą dane o swoich beneficjentach (Powiatowe Urzędy Pracy, Miejskie Ośrodki Pomocy Społecznej, Centrum Świadczeń Społecznych), funkcjonują w oparciu o dedykowane porozumienia administracyjne między instytucjami, regulujące cel i zakres współdziałania, w tym udostępniania danych. Instytucje te – posiadając własne bazy danych klientów, własne uregulowania dotyczące celu i zakresu przetwarzania danych, pełniąc jednocześnie rolę administratorów baz danych dla swoich baz danych – wymieniają między sobą dane tylko w uzasadnionych przypadkach. Podobnie wygląda tu współpraca z instytucjami zewnętrznymi (np. między Powiatowym Urzędem Pracy a Zakładem Ubezpieczeń Społecznych) – działanie w trybie wnioskowym. Tym samym nie jest możliwe sprawdzenie efektywności mechanizmu pomocowego, efektywności pomocy dla danego mieszkańca, ani wykrywanie nadużyć. Proponowana poprawka ma na celu wyeliminowanie tych bolączek i ułatwienie przekazywania danych między organami administracji publicznej.

# Jakie zmiany wprowadza nowelizacja 500+?

**Dwa typy administratorów danych:**

- Należący do sektora prywatnego, którymi są podmioty decydujące o celach i środkach przetwarzania danych osobowych
- Należący do sektora publicznego, którymi są podmioty decydujące o celach i środkach przetwarzania danych osobowych, przy czym te podmioty uważa się za jednego administratora danych jeżeli przetwarzanie danych służy temu samemu interesowi publicznemu

# Jeden ADO w administracji publicznej – jak to rozumieć? (1)

- **Jeden „zbiorowy” ADO, jeżeli przetwarzanie danych przez kilka organów „służy temu samemu interesowi publicznemu”**
  - Znajduje uznanie w ściśle językowej wykładni nowego brzmienia art. 23 ust. 2a UODO
  - Jest sprzeczne z Dyrektywą 95/46/WE i RODO (Rozporządzeniem 2016/679)
  - „proponowana poprawka ma na celu […] ułatwienie przekazywania danych między organami administracji publicznej” – nie mamy więc do czynienia z jednym zbiorowym administratorem (wykładnia autentyczna).

Jak taki zbiorowy administrator miałby działać?

# Jeden ADO w administracji publicznej – jak to rozumieć? (2)

- **Kilka organów, będących jednocześnie administratorem tych samych danych, jeżeli przetwarzanie ich „służy temu samemu interesowi publicznemu”**
  - Zgodne z dyrektywą 95/46/WE i rozporządzeniem 2016/679 (RODO)
  - ADO nadal jest „organ”, a nie np. grupa organów – nie zmieniono samej definicji administratora danych w UODO
  - Zgodnie z celem który przyświecał autorom art. 38 „Ustawy 500+” (chyba…)

# Problemy z interpretacją - przyczyny

- Pojęcie wspólnego administratora danych nie zostało nigdzie zdefiniowane
- Treść pojęcia interesu publicznego nie jest stała, zmienia się (np. w zależności od sytuacji politycznej, systemu wartości stosowanych w danym państwie)

**Interes publiczny** – wartości powszechnie uznawane za podstawowe i wspólne dla całego społeczeństwa (prof. Ciechanowicz – Prawo i polityka ochrony środowiska)

# Dlaczego to takie ważne?

*"Art. 7 Konstytucji Rzeczypospolitej Polskiej z 1997 r. stanowiący, że organy władzy publicznej działają na podstawie i w granicach prawa,*

- Charakter zmian jest systemowy
- Przekazywanie danych osobowych pomiędzy kilkoma organami administracji publicznej, będącymi administratorami tych danych, nie będzie już uznawane za udostępnienie danych osobowych, jeżeli ci administratorzy przetwarzają dane dla tego samego interesu publicznego
- Przekazywanie danych może się odbywać bez ograniczenia do sytuacji, gdy przewidują to przepisy prawa stanowiące podstawę dla przetwarzania danych

Nie zmieniono przy tym zasady adekwatności danych

# Powierzanie danych osobowych po zmianach „500+”

## Kiedy ADO może powierzyć dane ?

| | ADO ze sfery prawa prywatnego | ADO ze sfery prawa publicznego |
|---|---|---|
| **Przyjmujący** (procesor) ze sfery prawa prywatnego | Należy zawrzeć umowę powierzenia | Należy zawrzeć umowę powierzenia |
| **Przyjmujący** (procesor )ze sfery prawa publicznego | Należy zawrzeć umowę powierzenia | Brak obowiązku zawarcia umowy powierzenia |

# Wnioski i wątpliwości intepretacyjne

- Sprzeczne z dyrektywą 95/46/WE i rozporządzeniem 2016/679 (brak umowy)
- Skutkuje brakiem prawnego obowiązku zawierania jakiejkolwiek umowy w zakresie powierzenia przetwarzania danych pomiędzy podmiotami z sektora publicznego (brak umowy nie stanowi naruszenia przepisów o ochronie danych osobowych)
- Zgodnie z czysto językową wykładnią obowiązek zabezpieczenia danych dotyczy tylko podmiotów, które zawarły umowę na piśmie (rezultat tej wykładni niemożliwy do zaakceptowania ze względu na sprzeczność z przepisami dyrektywy 95/46/WE i rozporządzenia 2016/679).
- Co z nakazem ochrony danych przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną (kto jest uprawniony) ?
- Jak ustalić kto jest kim w procesie przetwarzania??

# Jak „widzi” to GIODO?

(..) Dlatego, stojąc na straży właściwego, wysokiego, standardu ochrony danych osobowych w Rzeczypospolitej Polskiej, organ do spraw ochrony danych osobowych będzie interpretował, dodane przez art. 38 ustawy o pomocy państwa w wychowywaniu dzieci, przepisy art. 23 ust. 2a oraz art. 31 ust. 2a ustawy o ochronie danych osobowych uwzględniając całokształt zaprezentowanych wyżej rozważań. Jednocześnie mając na względzie niezgodność konstrukcji prawnej przewidzianej w art. 23 ust. 2a z obowiązującym prawem europejskim Generalny Inspektor Ochrony Danych Osobowych będzie dążył do zmiany tego aktu prawnego.

**Źródło: http://www.giodo.gov.pl/560/id_art/9121/j/pl/**

# RODO

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)”

# Wybrane Nowości i zmiany Wprowadzone przez RODO

**Obowiązek określenia czasu przetwarzania danych**

- Jeżeli czas przetwarzania definiuje przepis prawa, administrator nie musi dodatkowo go określać
- Jeżeli czas przetwarzania nie jest określony w przepisach, administrator musi określić mając na uwadze cel przetwarzania czas po którym będzie dane usuwał,
- Czas przetwarzania uwzględniany jest w tzw. obowiązku informacyjnym
- Czas przetwarzania jest dokumentowany (Rejestr).

# Wybrane Nowości i zmiany Wprowadzone przez RODO

- Obowiązek uwzględnienia ochrony danych osobowych w fazie projektowania (privacy by design)
- Obowiązek wprowadzenia domyślnej ochrony danych osobowych (privacy by default)
- Obowiązek dokonywania oceny skutków planowanych operacji przetwarzania danych

# Wybrane Nowości i zmiany Wprowadzone przez RODO

## Obowiązek rejestrowania czynności przetwarzania danych

- Każdy administrator (…) prowadzą rejestr czynności przetwarzania danych osobowych, za które odpowiadają. W rejestrze tym zamieszcza się wszystkie następujące informacje:
  - (…) dane kontaktowe administratora (...)przedstawiciela administratora oraz DPO;
  - cele przetwarzania;
  - opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
  - kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione (…);
  - (…) przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej,
  - (…) planowane terminy usunięcia poszczególnych kategorii danych;
  - (…) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa,(…)
- Każdy podmiot przetwarzający (…) prowadzą rejestr (…), zawierający następujące informacje:
  - dane kontaktowe podmiotu przetwarzającego (…) oraz inspektora ochrony danych;
  - kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;
  - przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej
  - ogólny opis technicznych i organizacyjnych środków bezpieczeństwa

# Wybrane Nowości i zmiany Wprowadzone przez RODO

**Obowiązek rejestrowania czynności przetwarzania danych powstaje gdy administrator/podmiot przetwarzający:**

- zatrudnia więcej niż 250 osób (bez względu na formę zatrudnienia)
- przetwarzanie może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą,
- przetwarzanie nie ma charakteru sporadycznego
- przetwarzanie obejmuje szczególne kategorie danych osobowych,

# Wybrane Nowości i zmiany Wprowadzone przez RODO

**Obowiązek zgłaszania naruszenia ochrony danych osobowych (tak jak w telekomunikacji)**

- w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu (…) chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
- Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
- Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.

# Wybrane Nowości i zmiany Wprowadzone przez RODO

**Możliwość skonsultowania przetwarzania danych osobowych z organem nadzorczym.**

- Jeżeli ocena skutków dla ochrony danych, wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania administrator konsultuje się z organem nadzorczym.

# Wybrane Nowości i zmiany Wprowadzone przez RODO

**Obowiązek informowania podmiotu danych**

- Zmiana w obowiązku informacyjnym:
  - Dane kontaktowe Inspektora Ochrony Danych (DPO)
  - Podstawa prawna przetwarzania danych
  - Wyjaśnienie usprawiedliwionego celu
  - Zamiar przekazania danych do państwa trzeciego lub organizacji międzynarodowej
  - Okres przechowywania danych (lub kryteria jego ustalania)
  - Prawo cofnięcia zgody
  - Prawo wniesienia skargi do organu nadzorczego
  - Informacja o profilowaniu i automatycznych decyzjach

# Wybrane Nowości i zmiany Wprowadzone przez RODO

**Obowiązek ograniczenia przetwarzania danych**

- W wyjątkowych okolicznościach ADO będzie miał obowiązek „zawieszenia” przetwarzania danych klienta (np. na czas rozstrzygnięcia sporu na przetwarzanie danych).
- Jak ? Np.. poprzez:
  - przeniesienie wybranych danych osobowych do innego systemu przetwarzania,
  - uniemożliwienie użytkownikom dostępu do wybranych danych, lub
  - czasowe usunięcie opublikowanych danych ze strony internetowej

# Wybrane Nowości i zmiany Wprowadzone przez RODO

**Obowiązek informowania o usunięciu, sprostowaniu lub ograniczeniu przetwarzania danych**

- Właściciel danych będzie musiał zostać poinformowany w przypadku gdy dokonamy ww. operacji na jego danych
  - Sposób poinformowania nie wymaga zachowania formy pisemnej (dopuszczalna f. elektroniczna)

# Wybrane Nowości i zmiany Wprowadzone przez RODO

**Obowiązek zapewnienia środków technicznych i organizacyjnych aby zapewnić bezpieczeństwo danych osobowych – podejście od strony oceny ryzyka**

- Administrator danych nie otrzyma jak dotychczas „Rozporządzenia" z opisem jaki zakres powinna zawierać np. dokumentacja, jakiej długości ma być hasło uwierzytelniające do systemu i jak często zmieniane. Nowe podejście wymaga od Administratora danych ciągłej identyfikacji ryzyk jakie mogą się zmaterializować w trakcie procesów przetwarzania danych i doboru odpowiednich zabezpieczeń.
- RODO premiuje systemy oparte na:
  - **Kodeksach dobrych praktyk** (opracowanych np. dla danej branży, zaakceptowanych przez organy nadzoru (GIODO).
  - **Certyfikacji przez akredytowane jednostki certyfikujące** (Akredytacji może udzielić organ nadzoru w UE i PL).

# Wybrane Nowości i zmiany Wprowadzone przez RODO

**Obowiązek/brak obowiązku wyznaczenia inspektora ochrony danych (DPO - Data Protection Officer, dawny ABI)**

- RODO wprowadza obowiązkowość powołania DPO (Inspektora Ochrony Danych) w następujących przypadkach:
  - W każdym przypadku w podmiotach z sektora publicznego (wyjątek sądy w zakresie sprawowania wymiaru sprawiedliwości)
  - W niektórych przypadkach w podmiotach z sektora prywatnego
    - Gdy główna działalność (zasadnicze a nie poboczne czynności) polega na operacjach przetwarzania danych (…) na dużą skalę
    - Gdy przetwarza dane wrażliwe
  - DPO może być osoba:
    - ✓ Która ma odpowiednie kwalifikacje zawodowe, a w szczególności wiedzę fachową na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełniania zadań o których mowa w art. 39 (zabezpieczenia)
    - ✓ Ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych
    - ✓ Posiada odpowiednią wiedzę w zakresie ochrony danych osobowych
    - ✓ Nie była karana za umyślne przestępstwo
- RODO wprowadza możliwość wprowadzenia DPO przez „grupę przedsiębiorców (o ile będzie z nim można nawiązać kontakt z każdej jednostki organizacyjnej
- Jeżeli ADO jest organem publicznym – dla kilku takich organów lub podmiotów można wyznaczyć – z uwzględnieniem ich struktury organizacyjnej i wielkości – jednego Inspektora Ochrony Danych

# Wybrane Nowości i zmiany Wprowadzone przez RODO

**Brak obowiązku rejestrowania zbiorów danych osobowych**

- Obowiązek rejestracyjny zostaje całkowicie zniesiony (czy jest DPO czy go nie ma)
  - Nie oznacza to, że nie ma żadnych obowiązków dokumentacyjnych dla Administratora Danych (np. obowiązek prowadzenia dokumentacji operacji przetwarzania danych wymaga m.in. opisania zbiorów)

# Wybrane Nowości i zmiany Wprowadzone przez RODO

**Rozszerzone uprawnienia osoby, której dane dotyczą:**

- Prawo do informacji
- Prawo dostępu do danych
- Prawo do sprostowania danych
- Prawo do ograniczenia przetwarzania danych
- Prawo do bycia zapomnianym
- Prawo do przenoszenia danych

r.radko@tz-c.pl

# DZIĘKUJĘ ZA UWAGĘ