lubasz&wspólnicy

KANCELARIA RADCÓW PRAWNYCH

PARTNER

ETL | International

www.lubasziwspolnicy.pl

lubasz&wspólnicy
KANCELARIA RADCÓW PRAWNYCH

Ochrona danych osobowych w systemach informatycznych

Konferencja „Nowe regulacje w zakresie ochrony danych osobowych”
2 czerwca 2017 r.

Katarzyna Witkowska

Źródła prawa ochrony danych

Ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych - (dalej jako „UODO")

Rozporządzenie PE i Rady UE 2016/679 z dnia 27 kwietnia 2016 roku 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) – (dalej jako „RODO") – znajdzie zastosowanie od 25.05.2018 r.

Źródła prawa ochrony danych

Rozporządzenia Ministra Administracji i Cyfryzacji:

- **z dnia 11 maja 2015 roku w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych**
- **z dnia 11 maja 2015 roku w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji**
- **z dnia 10 grudnia 2014 roku w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji**

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych

Założenia rozporządzenia

Wysoki i spójny poziom ochrony osób fizycznych

Usunięcie przeszkód w przepływie danych osobowych

Technologiczna neutralność

Dostosowanie prawa do postępu technologicznego

Ujednolicenie poziomu obowiązków i zadań ADO i procesorów

Jak jest?

- **Polityka bezpieczeństwa**
- **Instrukcja zarządzania systemem informatycznym**

lubasz&wspólnicy
KANCELARIA RADCÓW PRAWNYCH

Polityka bezpieczeństwa – elementy

PB	**Wyciąg zasad dla użytkowników**	**Powołanie ABI/ASI**	**Wykaz zbiorów danych**	**Opis struktury zbiorów**
Lokalizacja przetwarzania	**Przepływ danych**	**Zastosowane środki techniczne i organizacyjne**	**Wzór upoważnień**	**Ewidencja upoważnień**
Plan szkoleń	**Lista osób przeszkolonych**	**Wzór umowy powierzenia**	**Wzór oświadczeń i umów o poufności**	**Plan sprawdzeń**
Wzór sprawozdania ze sprawdzenia	**Instrukcja alarmowa**	**Rejestr powierzeń i udostępnień**	**Wzory klauzul informacyjnych**	**Wzór rejestru ABI**

Instrukcja zarządzania systemem informatycznym zawiera m.in..

- procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności
- stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem
- procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu
- procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania
- procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych
- sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych

Poziomy zabezpieczeń DO w systemach informatycznych

podstawowy

- **w systemie informatycznym nie ma danych wrażliwych**
- **żadne z urządzeń służących do przetwarzania danych nie jest podłączone do sieci publicznej**

podwyższony

- **w systemie informatycznym są przetwarzane dane wrażliwe**
- **żadne z urządzeń służących do przetwarzania danych nie jest podłączone do sieci publicznej**

wysoki

- **przynajmniej jedno urządzenie służące do przetwarzania danych jest połączone z siecią publiczną**

Poziom wysoki

zabezpieczenie przed dostępem nieuprawnionych

kontrola dostępu do systemu, odrębne identyfikatory, dostęp po uwierzytelnieniu

system zabezpiecza się przed:

- **wirusami, programami szpiegującymi**
- **utratą danych spowodowaną awarią zasilania lub zakłóceniami sieci**

przy korzystaniu z komputerów przenośnych zachowanie szczególnej ostrożności przy ich transporcie i przechowywaniu

Poziom wysoki

identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie

zmiana haseł następuje nie rzadziej niż co 30 dni. Składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne

urządzenia i nośniki zawierające dane osobowe wrażliwe, które zabiera się poza obszar przetwarzania, zabezpiecza się w sposób zapewniający poufność i integralność tych danych

Poziom wysoki

kopie zapasowe:

- przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem;
- usuwa się niezwłocznie po ustaniu ich użyteczności.

urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

- likwidacji - pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
- przekazania podmiotowi nieuprawnionemu do przetwarzania danych - pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
- naprawy - pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

Poziom wysoki

System informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.

W przypadku zastosowania logicznych zabezpieczeń, o których mowa powyżej, obejmują one:

- **kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną;**
- **kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych**
- **Administrator danych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej**

Jak będzie?

Obowiązki

Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych

- ADO wdraża odpowiednie środki techniczne i organizacyjne
  - takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych
  - aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania

Nowe definicje

Pseudonimizacja - przetworzenie DO:

- **tak, by nie można ich było przypisać konkretnej osobie fizycznej**
- **Bez użycia dodatkowych informacji**

pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

Privacy by Design

Podejście proaktywne	**Prywatność włączona w projekt**	**Suma dodatnia**
Ochrona informacji przez cały cykl jej życia	**Transparentność i przejrzystość**	**Poszanowanie prywatności użytkowników**

Privacy by Default

Ochrona prywatności – ustawienie domyślne

Zmiana ustawień – na żądanie użytkownika

Zasada minimalizacji danych

Informacja

Szacowanie zagrożeń właściwych dla przetwarzania danych i ich skutków

Przed wdrożeniem zabezpieczeń ADO musi ocenić prawdopodobieństwo i wagę zagrożenia dla praw i wolności osoby, której dane dotyczą

- Co decyduje? – charakter, zakres, skala, sposób i cel przetwarzania, źródło danych osobowych
- Rozporządzenie zachowuje technologiczną neutralność
- Sprawdzone rozwiązania – zatwierdzone kodeksy postępowania, certyfikacja, wytyczne Europejskiej Rady Ochrony Danych,

Podatności

Awaria sprzętu	Błąd w systemie	Nieuprawnione użycie nośników danych	Dostęp nieuprawnionych użytkowników
Przekierowanie wiadomości	Nielegalne oprogramowanie	Kradzież	Awaria zasilania
Złośliwe oprogramowanie	Błąd użytkownika	Zużycie nośnika	Zalanie

Bezpieczeństwo przetwarzania

ADO i procesor wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić poziom bezpieczeństwa odpowiadający zagrożeniom – uwzględniając

- **pseudonimizację i szyfrowanie danych osobowych;**
- **zdolność do zapewnienia na bieżąco poufności, integralności, dostępności i odporności systemów i usług przetwarzających dane osobowe;**
- **zdolność do szybkiego przywrócenia dostępności danych i dostępu do nich w razie incydentu fizycznego lub technicznego;**
- **regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.**

Obowiązki

Rejestrowanie czynności przetwarzania

- ADO prowadzi rejestr podlegających mu czynności przetwarzania danych osobowych.
- W rejestrze tym zamieszcza się następujące informacje:
  - imię i nazwisko lub nazwę oraz dane kontaktowe ADO oraz wszelkich współadministratorów, 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,
  - planowane terminy usunięcia poszczególnych kategorii danych;
  - ogólny opis technicznych i organizacyjnych środków bezpieczeństwa;

Powierzenie (m. in. Hosting)

Możliwość korzystania z usług procesora

- O ile zapewnia on wystarczające wdrożenia odpowiednich środków

Zakaz dalszego powierzania bez zgody ADO

- Zgoda szczegółowa
- Zgoda ogólna pisemna

Przetwarzanie danych przez procesora

- Regulowane umową
- Lub innym aktem prawnym

Wymogi dla umowy / aktu prawnego

- Przedmiot i czas przetwarzania
- Charakter i cel przetwarzania
- Rodzaj DO i kategorie osób
- Obowiązki i prawa ADO

DZIĘKUJĘ ZA UWAGĘ!

Katarzyna Witkowska

katarzyna.witkowska@lubasziwspolnicy.pl
tel. kom.: + 48 512 987 244

Lubasz i Wspólnicy Kancelaria Radców Prawnych sp. k.
ul. Żwirki 17
90-539 Łódź