Tę i inne prezentacje - materiały konferencyjne tej Konferencji OSKKO – można znaleźć na stronie:
www.oskko.edu.pl/konferencjaoskko2018/ w zakładce: materiały do pobrania

OD ODO DO RODO

Kraków 02.03.2018

Tomasz Paprocki
FUSION 24
www.abifusion24.pl

Przepisy prawa Konstytucja RP

art. 47. Konstytucja RP

- Każdy ma prawo do ochrony życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.

art. 51. Konstytucja RP

- Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby.

Przepisy Prawa

- Ustawa o ochronie danych osobowych;
- Rozporządzenie w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;
- Rozporządzenie w sprawie zadań ABI;
- Rozporządzenie w sprawie wzoru zgłoszenia ABI do rejestracji;
- Rozporządzenie w sprawie prowadzenia rejestru przez ABI.
- Krajowe Ramy Interoperacyjności

RODO

- W maju 2016 roku opublikowany został tekst nowego
- Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych, czyli tzw. ogólne rozporządzenie o ochronie danych osobowych.

Przepisy Prawa

- ROZPORZĄDZENIE RADY MINISTRÓW
- z dnia 12 kwietnia 2012 r.
- w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych
- § 3. 1. Krajowe Ramy Interoperacyjności określają:
- 1) sposoby postępowania podmiotu realizującego zadania publiczne w zakresie doboru środków, metod i standardów wykorzystywanych do ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i udoskonalania systemu teleinformatycznego wykorzystywanego do realizacji zadań tego podmiotu oraz procedur organizacyjnych,.....:

Administrator Danych Osobowych

- DYREKTOR PLACÓWKI OŚWIATOWEJ SPRAWUJE FUNKCJĘ ADMINISTRATORA DANYCH
- ART. 7 PKT 4 U.O.D.O.
- ADMINISTRATOR DANYCH - TO ORGAN, JEDNOSTKA ORGANIZACYJNA, PODMIOT LUB OSOBA, O KTÓRYCH MOWA W ART. 3, DECYDUJĄCE O CELACH I ŚRODKACH PRZETWARZANIA DANYCH OSOBOWYCH

Administrator Danych Osobowych

- W związku z powyższym każda placówka edukacyjna jest, w rozumieniu ustawy, administratorem danych osobowych (ADO), zobowiązanym do stosowania środków technicznych i organizacyjnych, zapewniających ochronę przetwarzanych danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną

Administrator Danych Osobowych

- ADO jest w szczególności zobowiązany do zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
- Ma również obowiązek prowadzenia dokumentacji, opisującej sposób przetwarzania danych oraz środki ich ochrony.

Obowiązek informacyjny

- Zgodnie z art. 24 i 25 ustawy o ochronie danych osobowych (gdy dane zbierane są bezpośrednio od osoby, której dotyczą, jak też, gdy zbierane są pośrednio) na administratorze danych spoczywa obowiązek informacyjny. Chodzi o to, aby na podstawie uzyskanych informacji osoba, której dane dotyczą miała możliwość właściwego ocenienia sytuacji i podjęcia decyzji co do udostępnienia swoich danych, a także, aby mogła korzystać z praw wynikających z art. 32 ustawy

Do obowiązków informacyjnych, przewidzianych w art. 24 ustawy należą

- poinformowanie o adresie swojej siedziby i pełnej nazwie (art. 24 ust. 1 pkt 1),
- poinformowanie o celu zbierania danych, a w szczególności o znanych administratorowi danych osobowych, w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych (art. 24 ust. 1 pkt 2),
- poinformowanie o prawie dostępu do treści swoich danych oraz ich poprawiania (art. 24 ust. 1 pkt 3),
- poinformowanie o dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej (art. 24 ust. 1 pkt 4).

Art. 25. 1. W przypadku zbierania danych osobowych nie od osoby, której one dotyczą

- Art. 25. 1. W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych, o:
- 1) adresie swojej siedziby i pełnej nazwie, ...
- 2) celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych;
- 3) źródle danych;
- 4) prawie dostępu do treści swoich danych oraz ich poprawiania;

Klauzula obowiązku informacyjnego w przypadku pozyskania danych nie od osoby, której dane dotyczą

- Zgodnie z art. 25 ust. 1 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych, zwanej dalej ustawą, informuję, że:
- 1) administratorem Pani/Pana danych osobowych jest …….. z siedzibą w ……., zwana dalej ……,
- 2) Pani/Pana dane osobowe przetwarzane będą w celu ……. i nie będą udostępniane innym odbiorcom,
- 3) ……. pozyskała Pani/Pana dane osobowe od …… z siedzibą w ……,
- 4) posiada Pani/Pan prawo dostępu do treści swoich danych oraz ich poprawiania,
- 5) na podstawie art. 32 ust. 1 pkt 7 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn.: Dz.U. z 2016 r. poz. 922) przysługuje Pani/Panu prawo wniesienia pisemnego, umotywowanego żądania zaprzestania przetwarzania Pani/Pana danych ze względu na Pani/Pana szczególną sytuację, jak również – na podstawie art. 32 ust. 1 pkt 8 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn.: Dz.U. z 2016 r. poz. 922) ma Pani/Pan prawo wniesienia sprzeciwu wobec przetwarzania Pani/Pana danych w celach marketingowych lub wobec przekazywania ich innemu administratorowi danych.

Klauzula obowiązku informacyjnego zamieszczana w treści umowy z pracownikiem

- Zgodnie z art. 24 ust. 1 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych informuję, że administratorem Pani/Pana danych osobowych jest ……. z siedzibą …….. Dane osobowe będą przetwarzane w celach związanych z zawarciem i realizacją umowy o pracę. W razie takiej konieczności dane mogą być udostępniane podmiotom z grupy ……., podmiotom udzielającym świadczenia zdrowotne, podmiotowi organizującemu szkolenia w zakresie bhp, zakładom ubezpieczeń i brokerom ubezpieczeniowym, podmiotom wydającym karty sportowe, podmiotom wydającym służbowe karty debetowe lub kredytowe oraz innym podmiotom upoważnionym na podstawie przepisów prawa.
- Przysługuje Pani/Panu prawo dostępu do treści swoich danych oraz ich poprawiania. Podanie danych jest obowiązkowe i wynika z przepisów prawa pracy, tj. w szczególności art. 221 Kodeksu pracy oraz przepisów rozporządzenia ministra pracy i polityki socjalnej z 28 maja 1996 r. w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika.

Obowiązek informacyjny CV

- Dość często administratorzy danych próbują realizować obowiązek informacyjny w formie niżej przedstawionej klauzuli, która została przekopiowana z serwisu rekrutacyjnego:
- **„Wyrażam zgodę na przetwarzanie moich danych osobowych dla potrzeb niezbędnych do realizacji procesu rekrutacji (zgodnie z Ustawą z dnia 29.08.1997 roku o Ochronie Danych Osobowych; tekst jednolity: Dz. U. 2016 r. poz. 922)”.**

- **Przedstawiona klauzula informacyjna zawiera rażące braki formalne:**
- **nie został wskazany administrator danych (art. 24 ust. 1 pkt 1 uodo);**
- **brakuje informacji o celu przetwarzania danych oraz przewidywanych odbiorcach lub kategoriach odbiorców (art. 24 ust. 1 pkt 2 uodo);**
- **nie ma informacji o prawie dostępu do treści swoich danych oraz ich poprawienia (art. 24 ust. 1 pkt 3 uodo);**
- **brakuje informacji o dobrowolności podania danych (art. 24 ust. 1 pkt 4 uodo).**
- **Wyrażenie zgody na przetwarzanie danych przez osobę, której one dotyczą, nie jest tożsame ze spełnieniem obowiązku informacyjnego przez administratora danych.**
- **Na gruncie uodo to dwie zupełnie różne instytucje.**
- ***W takim przypadku dochodzi do naruszenia przepisów o ochronie danych osobowych na płaszczyźnie realizacji obowiązku informacyjnego oraz w sferze możliwości wykonywania przez podmiot danych swoich uprawnień w zakresie kontroli przetwarzania jej danych, o których mowa w art. 32 i n. uodo.***

Klauzula obowiązku informacyjnego w procesie rekrutacji

- CV kandydatów nierozpatrzone w danym procesie rekrutacji są przechowywane przez okres …….. na potrzeby kolejnych procesów rekrutacji. Po tym okresie są usuwane, a dane osobowe kandydatów nie są przetwarzane w żadnym innym celu.
  Aplikacji nie odsyłamy. Kontaktujemy się jedynie z wybranymi osobami. Osoby zainteresowane udziałem w kolejnych i podobnych procesach rekrutacji prosimy o zamieszczenie w swoim CV klauzuli o treści:

- Wyrażam zgodę na przetwarzanie moich danych osobowych przez Szkołę Podstawową nr X w Rxxxxxxxx, ul. XXXXXXXXXX, 00-000 Rxxxxxxx, zawartych w CV na potrzeby obecnego oraz przyszłych procesów rekrutacji. Zgodnie z Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych Dz. U. 2016 r. poz. 922.

- Zgodnie z Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2016 r. poz. 922.) wyrażam zgodę na przetwarzanie moich danych osobowych. Administratorem danych osobowych jest Szkoła Podstawowa nr X w Rxxxxxxxxx, ul. Xxxxxxxxxxxx. Przysługuje mi prawo wglądu do treści danych oraz ich uaktualniania czy sprostowania w razie stwierdzenia, że dane są niekompletne, nieaktualne lub nieprawdziwe. Dane podaję dobrowolnie.

Podpis data ……

Klauzula obowiązku informacyjnego w procesie rekrutacji

- CV kandydatów nierozpatrzone w danym procesie rekrutacji są przechowywane przez okres …….. na potrzeby kolejnych procesów rekrutacji. Po tym okresie są usuwane, a dane osobowe kandydatów nie są przetwarzane w żadnym innym celu. Aplikacji nie odsyłamy. Kontaktujemy się jedynie z wybranymi osobami. Osoby zainteresowane udziałem w kolejnych i podobnych procesach rekrutacji prosimy o zamieszczenie w swoim CV klauzuli o treści:
- Wyrażam zgodę na przetwarzanie moich danych osobowych przez ……. z siedzibą w …….. zawartych w CV na potrzeby obecnego oraz przyszłych procesów rekrutacji.

Kryptografia danych przesyłanych w sieci publicznej

- Zgodnie z art. 36 ustawy administrator danych ma obowiązek zabezpieczenia danych m.in. przed ich nieuprawnionym ujawnieniem. W razie przesyłania danych metodą teletransmisji przy użyciu sieci publicznej zawsze istnieje możliwość przejęcia przesyłanych danych przez osobę nieuprawnioną. Istnieje również niebezpieczeństwo ich nieuprawnionej zmiany, uszkodzenia lub zniszczenia. Niezbędne jest zatem zastosowanie odpowiednich zabezpieczeń, które ochronią przesyłane dane.

Kryptografia danych przesyłanych w sieci publicznej

Umowy powierzenia danych osobowych oraz upoważnienia do ich przetwarzania

- Zgodnie z art. 37 ustawy do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych osobowych.
- Ponadto, zgodnie z art. 31 ustęp 1, administrator danych osobowych może powierzyć przetwarzanie danych innemu podmiotowi, w drodze umowy zawartej na piśmie

Umowy powierzenia danych osobowych oraz upoważnienia do ich przetwarzania

- W związku z powyższym ADO musi upoważnić do przetwarzania wszystkie osoby mające dostęp do danych osobowych. W praktyce dotyczyć to będzie wszystkich pracowników.
- Natomiast umowy powierzenia administrator danych musi zawrzeć z podmiotami zewnętrznymi, takimi jak firmy: dostawcy oprogramowania (z uwagi na umowę serwisową), e-dziennik itp..

Klauzula dotycząca kontroli wykonywania umowy przez procesora

- 1. Administrator jest uprawniony do kontrolowania sposobu wykonania umowy o powierzenie danych osobowych przez procesora oraz przestrzegania obowiązujących przepisów prawa z zakresu ochrony danych osobowych.
- 2. W celu wykonania kontroli upoważnieni pracownicy administratora mają prawo:
- 1) wstępu do pomieszczeń, w których procesor przetwarza powierzone dane osobowe, żądania złożenia pisemnych i ustnych wyjaśnień w celu ustalenia stanu faktycznego,
- 2) przeprowadzenia oględzin dokumentów, a także urządzeń, nośników oraz systemów informatycznych służących do przetwarzania powierzonych danych.

Klauzula umożliwiająca podpowierzenie danych osobowych

- Zleceniobiorca może, w celu prawidłowego wykonania umowy, zlecić osobom trzecim (w szczególności podwykonawcom) wykonywanie niektórych czynności wchodzących w zakres czynności przetwarzania danych osobowych powierzonych przez Zleceniodawcę (podpowierzenie przetwarzania danych osobowych), na podstawie odrębnej umowy, sporządzonej w formie pisemnej.

Umowy powierzenia danych osobowych oraz upoważnienia do ich przetwarzania

- Wraz z zbieraniem upoważnień należy pamiętać, zgodnie z art. 39 ustawy, o obowiązku prowadzenia ewidencji osób upoważnionych zgodnie. Ewidencja powinna zawierać:

- imię i nazwisko osoby upoważnionej,
- datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych,
- identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

- 1. Upoważniam Panią/Pana
- o numerze PESEL/numerze dowodu osobistego
- zatrudnioną/-ego na stanowisku
- w ……
- do dostępu do następujących zbiorów danych osobowych w celu ich przetwarzania:
- (Zbiór danych osobowych „ZBIÓR DANYCH PRACOWNIKÓW”)
- (W, WG, M, A,KS,KZ,KBHP)
- WG – wgląd, W – wprowadzanie, M – modyfikacja, U – usuwanie, A – archiwizacja
- KS-Komisja Socjalna, KZ-Komisja Zdrowotna, KBHP- Komisja BHP ,
- . Identyfikator/Login:

Zabezpieczenia systemów informatycznych

- stosowanie mechanizmów kontroli dostępu (jeżeli dostęp do systemu informatycznego posiadają co najmniej dwie osoby, wówczas każdy z użytkowników otrzymuje odrębny identyfikator, a dostęp uwarunkowany jest wprowadzeniem identyfikatora i dokonaniem uwierzytelnienia przy pomocy hasła składającego się co najmniej z ośmiu znaków, małych i wielkich liter oraz cyfr lub znaków specjalnych),
- zabezpieczenie przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego,
- zabezpieczenie przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej,
- identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie,

Zabezpieczenia systemów informatycznych

- wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych,
- przechowywanie kopii zapasowych w miejscach zabezpieczonych przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem,
- usuwanie kopii zapasowych niezwłocznie po ustaniu ich użyteczności,
- stosowanie środków ochrony kryptograficznej wobec sprzętu i nośników przenośnych,
- stosowanie środków ochrony przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem,
- monitorowanie wdrożonych zabezpieczeń w systemach informatycznych.

Ochrona stacji roboczych pracowników

- Stosowanie oprogramowania antywirusowego na stanowisku lokalnym
- Ograniczenie praw użytkowników- pracownik powinien pracować z ograniczonymi prawami w systemie, natomiast prawa administracyjne powinna mieć osoba(y) oddelegowana do zarzadzania stanowiskami roboczymi
- Zablokowanie możliwości instalowania oraz uruchamiania programów innych niż dozwolone (biała lista oprogramowania)
- Wymuszanie stosowania bezpiecznych połączeń i brak możliwości podłączania do obcych sieci

- Podczas audytów ochrony danych osobowych często pytamy kontrolowane podmioty o występowanie u nich incydentów związanych z ochroną danych osobowych czy bezpieczeństwem informacji. Zazwyczaj padają odpowiedzi, że nic takiego nie miało miejsca.

RODO

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)

Jak RODO definiuje administratora danych ?

- Artykuł 4 rozporządzenia stanowi:
- „(…) administratorem jest osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Natomiast jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania”.

OBOWIĄZEK INFORMACYJNY ZGODNY Z RODO

OBOWIĄZEK INFORMACYJNY ZGODNY Z RODO

- W przypadku, gdy zbieramy dane osobowe, od osoby której dane dotyczą zgodnie z art. 13 ust. 1 i 2 RODO powinniśmy poinformować ją o:
- a) swojej tożsamości i danych kontaktowych oraz tożsamość i danych kontaktowych swojego przedstawiciela, jeżeli istnieje;
- b) danych kontaktowy inspektora ochrony danych - nowość
- c) celach przetwarzania, do których mają posłużyć dane osobowe,
- d) podstawie prawnej przetwarzania; – nowość

OBOWIĄZEK INFORMACYJNY ZGODNY Z RODO

- f) prawnie uzasadnionym interesie realizowanym przez administratora lub przez stronę trzecią – jeżeli przetwarzanie odbywa się na podstawie prawnie usprawiedliwionego interesu ADO (art. 6 ust. 1 lit. f) **nowość**
- g) odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;

OBOWIĄZEK INFORMACYJNY ZGODNY Z RODO

- h) transferze danych do państwa trzeciego, w tym o:

- zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – **nowość**

OBOWIĄZEK INFORMACYJNY ZGODNY Z RODO

- i) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu; – nowość
- j) prawie do:
- żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą,
- ich sprostowania, usunięcia lub ograniczenia przetwarzania lub
- wniesienia sprzeciwu wobec przetwarzania, a także
- przenoszenia danych; – nowość

OBOWIĄZEK INFORMACYJNY ZGODNY Z RODO

- k) prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem jeżeli przetwarzanie odbywa się na podstawie zgody na przetwarzanie danych zwykłych (art. 6 ust. 1 lit. RODO) lub szczególnej kategorii (art. 9 ust. 2 lit. a) RODO). – nowość
- l) prawie wniesienia skargi do organu nadzorczego; – nowość

OBOWIĄZEK INFORMACYJNY ZGODNY Z RODO

- W przypadku, gdy zbieramy dane osobowe, od innego źródła niż od osoby której dane dotyczą zgodnie z art. 14 ust. 1 i 2 RODO powinniśmy poinformować ją o: źródle pochodzenia danych osobowych, a jeżeli ma to zastosowanie, o pochodzeniu ich ze źródeł powszechnie dostępnych
- Powyższe informacje administrator danych powinien przekazać w formie zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej oraz jasnym i prostym językiem w szczególności gdy informacje są kierowane do dziecka (art. 12 ust. 1 RODO).

Przykładowa treść klauzuli informacyjnej przy zbieraniu danych osobowych w procesie rekrutacyjnym zgodnie z RODO:

- Administratorem Twoich danych osobowych jest… z siedzibą przy ul. … w … Dane kontaktowe inspektora ochrony danych: abi@… Dane osobowe są przetwarzane w celu realizacji procesu rekrutacji, na podstawie Twojej dobrowolnej zgody. Masz prawo do wycofania zgody w dowolnym momencie, przy czym cofnięcie zgody nie ma wpływu na zgodność przetwarzania, którego dokonano na jej podstawie przed cofnięciem zgody. Dane osobowe będą przetwarzane aż do ewentualnego wycofania przez Ciebie zgody na przetwarzanie danych w procesie rekrutacji, nie dłużej jednak niż do zakończenia rekrutacji, w której bierzesz udział. Twoje dane osobowe mogą być przekazywane do państw trzecich, które zapewniają odpowiedni stopień ochrony Twoich danych osobowych. Podanie danych jest dobrowolne, ale konieczne w celu przeprowadzenia rekrutacji, w której bierzesz udział. Masz prawo dostępu do Twoich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do przenoszenia danych oraz prawo wniesienia skargi do organu nadzorczego”.

Przykładowa treść zgody w procesie rekrutacyjnym zgodnie z RODO:

- „Wyrażam zgodę na przetwarzanie moich danych osobowych zawartych w życiorysie dla celów prowadzonej przez ....w.... Rekrutacji na stanowisko..... Zostałem /zostałam poinformowany/a ,że wyrażenie zgody jest dobrowolne oraz ,że mam prawo do wycofania zgody w dowolnym momencie, a wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na jej podstawie przed jej wycofaniem ....”

Prawa podmiotów danych

- Prawo do bycia zapomnianym
- Prawo do przenoszenia danych
- Prawo sprzeciwu
- Prawo dostępu do danych i uzyskania kopii
- Prawo do niepodlegania profilowaniu

PRAWA PODMIOTÓW RODO

Obowiązek informacyjny – chcesz moje dane, powiedz mi po co?

- Kto będzie przetwarzał moje dane?
- W jakim celu?
- Jakie są moje prawa?
- Czy mam obowiązek podania danych, a jeśli tak, to z czego on wynika?
- Dane kontaktowe inspektora ochrony danych
- Zamiar przekazania danych osobowych do państwa trzeciego
- Okres przechowywania danych
- Profilowanie

Zgoda dziecka na przetwarzanie danych osobowych w świetle ogólnego rozporządzenia o ochronie danych

- Ogólne rozporządzenie o ochronie danych osobowych, które od 25 maja 2018 r. ujednolici zasady ochrony danych osobowych we wszystkich państwach członkowskich UE, stanowi, że korzystanie przez dzieci poniżej 16 roku życia z usług społeczeństwa informacyjnego, a więc m.in. portali społecznościowych i innych usług internetowych, będzie możliwe dopiero po wyrażeniu lub zaaprobowaniu takiej zgody przez rodziców albo opiekunów prawnych. Przewiduje jednak, że państwa członkowskie mogą w swoim prawie ustanowić niższą granicę wiekową – musi ona jednak wynosić co najmniej 13 lat.

OBOWIĄZEK INFORMACYJNY ZGODNY Z RODO

- MONITORING PROWADZONY JEST CAŁODOBOWO W CELU ZAPEWNIENIA BEZPIECZEŃSTWA W XXXXXXXXXXXXXXXXXXXXXXXXXXXX.
ADMINISTRATOREM DANYCH OSOBOWYCH W SYSTEMIE MONITORUJĄCYM JEST XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
OBSZAR MONITORINGU OBEJMUJE WEWNETRZNY I ZEWNĘTRZNY TEREN XXXXXXXXXXXXX.
WIĘCEJ INFORMACJI UZYSKAĆ MOŻNA W XXXXXXXXXX

Monitoring wizyjny

- Trzeba będzie określić w drodze odpowiedniej polityki zasady prowadzenia monitoringu, jak są przechowywane dane, kto ma do nich dostęp, kiedy są usuwane i w jaki sposób

Zabezpieczanie dokumentacji przekazywanej drogą elektroniczną

- Organ nadzorczy jasno wskazał na co będzie zwracał uwagę. Szybko wypunktuję:

- Czy jest prawidłowa autoryzacja (podpis elektroniczny / profil zaufany – identyfikacja)
- Czy podmiot, który powinien odebrać faktycznie odebrał (potwierdzenie dla celów dowodowych)
- Czy jest zachowana poufność transamisji (dane w transporcie czy są szyfrowane)

Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu (RODO)

Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu RODO

- Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu
- 1. W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, **nie później niż w terminie 72 godzin po stwierdzeniu naruszenia** – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych

Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu RODO

- Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:
- a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
- b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;

Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu RODO

- c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
- d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych RODO

- Artykuł 34
- Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych
- 1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

administracyjne kary pieniężne od 25 maja 2018

Artykuł 83 RODO

- Ogólne warunki nakładania administracyjnych kar pieniężnych
- 1. Każdy organ nadzorczy zapewnia, by stosowane na mocy niniejszego artykułu za naruszenia niniejszego rozporządzenia administracyjne kary pieniężne, o których mowa w ust. 4, 5 i 6, były w każdym indywidualnym przypadku:
- skuteczne, proporcjonalne i odstraszające.

Administracyjne kary pieniężne UODO (Projekt)

- Rozdział 9
- Administracyjne kary pieniężne
- Art. 83.1. Na podmioty publiczne, o których mowa w art. 9 pkt 1 – 12 i 14 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych Prezes Urzędu może nałożyć, w drodze decyzji, administracyjne kary pieniężne w wysokości do 100 000 zł.

Fundusz Ochrony Danych Osobowych

- Art. 98. 1. Tworzy się Fundusz Ochrony Danych Osobowych, zwany dalej „Funduszem”, którego dysponentem jest Prezes Urzędu.
- 2. Fundusz jest państwowym funduszem celowym.
- 3. Przychodami Funduszu są środki finansowe pochodzące z 1% kar pieniężnych nakładanych przez Prezesa Urzędu. Środku z Funduszu nie mogą być podstawą osiągania przychodu przez pracowników Urzędu

Administracyjne Kary Pieniężne

- Administracyjne kary pieniężne nakłada się, zależnie od okoliczności każdego
- Decydując, czy nałożyć administracyjną karę pieniężną, oraz ustalając jej wysokość, zwraca się w każdym indywidualnym przypadku należytą uwagę na:

- a) charakter, wagę i czas trwania naruszenia przy uwzględnieniu charakteru, zakresu lub celu danego przetwarzania, liczby poszkodowanych osób, których dane dotyczą, oraz rozmiaru poniesionej przez nie szkody;
- b) umyślny lub nieumyślny charakter naruszenia;
- c) działania podjęte przez administratora lub podmiot przetwarzający w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą;

- d) stopień odpowiedzialności administratora lub podmiotu przetwarzającego z uwzględnieniem środków technicznych i organizacyjnych wdrożonych przez nich na mocy art. 25 i 32;
- e) wszelkie stosowne wcześniejsze naruszenia ze strony administratora lub podmiotu przetwarzającego;
- f) stopień współpracy z organem nadzorczym w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków;
- g) kategorie danych osobowych, których dotyczyło naruszenie;

- h) sposób, w jaki organ nadzorczy dowiedział się o naruszeniu, w szczególności, czy i w jakim zakresie administrator lub podmiot przetwarzający zgłosili naruszenie;
- i) jeżeli wobec administratora lub podmiotu przetwarzającego, których sprawa dotyczy, zostały wcześniej zastosowane w tej samej sprawie środki, o których mowa w art. 58 ust. 2 – przestrzeganie tych środków;
- j) stosowanie zatwierdzonych kodeksów postępowania na mocy art. 40 lub zatwierdzonych mechanizmów certyfikacji na mocy art. 42; oraz
- k) wszelkie inne obciążające lub łagodzące czynniki mające zastosowanie do okoliczności sprawy, takie jak osiągnięte bezpośrednio lub pośrednio w związku z naruszeniem korzyści finansowe lub uniknięte straty.

Przepisy Karne w RODO

- Artykuł 82
- Prawo do odszkodowania i odpowiedzialność
- 1. Każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę

INSPEKTOR OCHRONY DANYCH

ABI
Administrator Bezpieczeństwa Informacji

- Art. 36a. 1. Administrator danych może powołać administratora bezpieczeństwa informacji.
- Art. 36a. 4. Administrator danych może powierzyć administratorowi bezpieczeństwa informacji wykonywanie innych obowiązków, jeżeli nie naruszy to prawidłowego wykonywania zadań, o których mowa w ust. 2

Inspektor Ochrony Danych IOD/DPO

- Nowe przepisy istotnie wzmacniają rolę i pozycję inspektorów ochrony danych. Jednym z najważniejszych przejawów tego wzmocnienia jest fakt, że wyznaczenie inspektora ochrony danych, stanie się w wielu przypadkach obowiązkiem, a nie jak dotąd, uprawnieniem administratora danych.

Artykuł 38 RODO
Status inspektora ochrony danych

- 1. Administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.
- 2. Administrator oraz podmiot przetwarzający wspierają inspektora ochrony danych w wypełnianiu przez niego zadań, o których mowa w art. 39, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej

Artykuł 38
Status inspektora ochrony danych

- Administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.
- 2. Administrator oraz podmiot przetwarzający wspierają inspektora ochrony danych w wypełnianiu przez niego zadań, o których mowa w art. 39, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.

- 3. Administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań.
- Nie jest on odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań.
- Inspektor ochrony danych bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego.

- 4. Osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia.
- 5. Inspektor ochrony danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań – zgodnie z prawem Unii lub prawem państwa członkowskiego.
- 6. Inspektor ochrony danych może wykonywać inne zadania i obowiązki. Administrator lub podmiot przetwarzający zapewniają, by takie zadania i obowiązki nie powodowały konfliktu interesów.

ABI
IOD/DPO

- Art. 36a. 5. Administratorem bezpieczeństwa informacji może być osoba, która:
- 1) ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych;
- 2) posiada odpowiednią wiedzę w zakresie ochrony danych osobowych;
- 3) nie była karana za umyślne przestępstwo.

- Art. 37 5. Inspektor ochrony danych jest wyznaczany
- 1)na podstawie kwalifikacji zawodowych,
- 2) wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych
- 3)umiejętności wypełnienia zadań, o których mowa w art. 39

Inspektor Ochrony Danych
Nowa Ustawa ODO

- Art. 5.
- 1 Administrator danych albo podmiot przetwarzający, który wyznaczył inspektora ochrony danych, zwanego dalej „inspektorem”, zawiadamia Prezesa Urzędu Ochrony Danych Osobowych, zwanego dalej „Prezesem Urzędu”, o jego wyznaczeniu, w terminie **14 dni** od dnia wyznaczenia, wskazując imię, nazwisko, adres poczty elektronicznej lub numer telefonu inspektora.
- 3. O każdej zmianie danych, o której mowa w ust. 1 i 2, w tym o odwołaniu inspektora, należy zawiadomić Prezesa Urzędu w terminie **14 dni** od dnia zaistnienia zmiany.

Inspektor Ochrony Danych

- Kwalifikacje do pełnienia funkcji
- Zgodnie z art. 37 ust. 5 RODO inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39 RODO. Poziom wiedzy inspektora powinien być ustalany w kontekście konkretnych potrzeb administratora danych i procesora (motyw 97 RODO).

- Zgodnie z Wytycznymi dotyczących inspektorów danych osobowych Grupy Roboczej art. 29 inspektor ochrony danych powinien posiadać odpowiednią wiedzę z zakresu krajowych i europejskich przepisów o ochronie danych osobowych i praktyk, jak również dogłębną znajomość przepisów RODO. Zalecana jest również wiedza biznesowa i sektorowa dotycząca działalności administratora.
- DPO powinien również posiadać odpowiednią wiedzę na temat procesów przetwarzania danych, systemów informatycznych oraz zabezpieczeń stosowanych u administratora i jego potrzeb w zakresie ochrony danych.
- W przypadku organów i podmiotów publicznych DPO powinien również wykazywać się znajomością procedur administracyjnych i funkcjonowania jednostki.

Grupa Robocza art. 29

- Znaczenie fachowej, a zatem stale uaktualnianej wiedzy DPO zostało podkreślone przez zobowiązanie administratorów danych i procesorów do zapewnienia inspektorowi zasobów niezbędnych do utrzymania jego wiedzy fachowej, a zatem systematycznego podnoszenia poziomu jego wiedzy. Wymóg uaktualniania wiedzy i zapewnienia na to środków finansowych jest uzasadniony wobec zmieniającego się stale stanu wiedzy technicznej, rozwoju technologicznego i postępu wielkoskalowych metod przetwarzania danych.
- Z pewnością można twierdzić, że w funkcję inspektora ochrony danych wpisane jest ciągłe kształcenie się, uwzględnianie zmian w prawie oraz zmian w metodach przetwarzania danych.

Zakres zadań inspektora ochrony danych zawiera art. 39 ust. 1 RODO

- 1) Informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
- 2) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
- 3) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35;
- 4) współpraca z organem nadzorczym

Zakres zadań inspektora ochrony danych zawiera art. 39 ust. 1 RODO

- 5) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;
- 6) pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia.
- 7) prowadzenie rejestru czynności lub rejestru kategorii czynności

Zasada rozliczalności – zmiana podejścia

- Dla zapewnienia najwyższego poziomu bezpieczeństwa administrator został zobowiązany do wprowadzenia kontroli przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną.

Co ADO musi wiedzieć o RODO

NOWE OBOWIĄZKI ADO,DPO

- **OCENA SKUTKÓW DLA OCHRONY DANYCH (privacy impact assessment)**
- **UWZGLĘDNIANIE PRYWATNOŚCI W FAZIE PROJEKTOWANIA**

(privacy by design)

- **W USTAWIENIACH DOMYŚLNYCH**

(privacy by default)

Co ADO musi wiedzieć o RODO

- Nowe obowiązki ADO,DPO
- Analiza ryzyka
- Rejestrowanie czynności przetwarzania
- Współpraca z organem nadzorczym- GIODO
- Odpowiednie zabezpieczenie danych
- Zgłaszanie naruszeń do organu nadzorczego- GIODO (72 godziny od stwierdzenia naruszenia)
- ADO musi poinformować GIODO ,że doszło do naruszenia ochrony danych w Twojej strukturze
- Zawiadomienie podmiotów danych o naruszeniu
- Ocena skutków dla ochrony danych
- Uprzednie konsultacje

Co ADO musi wiedzieć o RODO

Czego już nie będzie

- Sformalizowanej dokumentacji :
  Polityki, Instrukcji, rejestru, itp.
- Zgłaszania zbiorów
- Rejestru zbiorów ABI
- Zmiany haseł co 30 dni

- ISTOTNĄ NOWOŚCIĄ JEST RÓWNIEŻ REZYGNACJA Z WYMOGU PROWADZENIA WYKAZU ZBIORÓW DANYCH JAKO ELEMENTU POLITYKI BEZPIECZEŃSTWA ORAZ OBOWIĄZKU ZGŁASZANIA ZBIORÓW DANYCH DO REJESTRACJI GIODO.
- NA GRUNCIE RODO ZOSTAŁY ONE ZASTĄPIONE OBOWIĄZKIEM
- REJESTROWANIA CZYNNOŚCI PRZETWARZANIA DANYCH.

Tę i inne prezentacje - materiały konferencyjne XV Konferencji OSKKO - można znaleźć na stronie: **www.oskko.edu.pl/konferencjaoskko2018/** w zakładce: materiały do pobrania

DIEKUJĘ ZA UWAGĘ

Tomasz Paprocki
FUSION 24
www.abifusion24.pl