erasmus+

ZMIENIA ŻYCIE, OTWIERA UMYSŁY

www.erasmusplus.org.pl

frse
Fundacja Rozwoju Systemu Edukacji

Erasmus+

erasmus+

NA WAŻNY TEMAT

NARZĘDZIA PRAWNE I TECHNICZNE W UPOWSZECHNIANIU REZULTATÓW PROJEKTÓW EDUKACYJNYCH

www.erasmusplus.org.pl/upowszechnianie

DANE OSOBOWE UCZESTNIKÓW PROJEKTÓW ERASMUS+ A RODO

Jarosław Petz, SAR

O CZYM BĘDĘ MÓWIŁ?

1. Wprowadzenie do ochrony danych osobowych
2. Zbiory danych;
3. Proces ochrony danych i jego rozliczalność;
4. Wymagania techniczno-organizacyjno-formalne;
5. Przetwarzanie danych kadrowych, podwykonawców i uczestników projektów
6. Powierzanie danych osobowych do przetwarzania;
7. Zgłaszanie Organowi Nadzorczemu naruszeń ochrony danych;
8. Odpowiedzialność prawna;

Wprowadzenie do ochrony danych osobowych

ŹRÓDŁA WYMAGAŃ DOTYCZĄCYCH BEZPIECZEŃSTWA INFORMACJI

- Konstytucja RP: art. 47 art. 51
- Ustawa o ochronie danych osobowych: art. 1
- Rozporządzenie w sprawie dokumentacji i przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych
- Rozporządzenia wykonawcze MAiC
- Rozporządzenie w sprawie Krajowych Ram Interoperacyjności (KRI), minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych
- System Zarządzania Bezpieczeństwem Informacji w KRI
- Ustawy samorządowe (województwo, gmina, powiat)

ŹRÓDŁA WYMAGAŃ DOTYCZĄCYCH BEZPIECZEŃSTWA INFORMACJI

- Przepisy szczególne w administracji publicznej (np. Centra Usług Wspólnych)
- Ustawa Prawo Pracy (art. 221)
- Ustawa o ochronie informacji niejawnych
- Ustawa Prawo zamówień publicznych
- Ustawa o dostępie do informacji publicznej *{o jawności życia publicznego}*
- Ustawa o świadczeniu usług drogą elektroniczną (art.9-10, 16-22) *{ePrivacy}*
- Ustawa Ordynacja Podatkowa

ŹRÓDŁA WYMAGAŃ DOTYCZĄCYCH BEZPIECZEŃSTWA INFORMACJI

- Ustawa Prawo Telekomunikacyjne (art.173-174)
- Ustawa o swobodzie działalność gospodarczej
- Ustawa o Ochronie Baz Danych
- Ustawa o Prawie Autorskim i Prawach Pokrewnych
- Pakiet przepisów konsumenckich
- Kodeksy: Karny, Administracyjny i Cywilny
- Przepisy i normy branżowe np. medyczne, szkolnictwo, ubezpieczeniowe, …

ŹRÓDŁA WYMAGAŃ DOTYCZĄCYCH BEZPIECZEŃSTWA INFORMACJI

REGULACJE WEWNĘTRZNE

Polityka Bezpieczeństwa Danych Osobowych

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

Instrukcja postepowania w sytuacji naruszenia ochrony danych osobowych

Polityka Bezpieczeństwa IT

INFORMACJE PRAWNIE CHRONIONE

Tajemnice zawodowe,

Tajemnice przedsiębiorstwa, pracodawcy,

Tajemnica pracownika samorządowego,

Tajemnica skarbowa,

Informacje niejawne

ŹRÓDŁA WYMAGAŃ DOTYCZĄCYCH BEZPIECZEŃSTWA INFORMACJI

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

RODO Rozporządzenie o Ochronie Danych Osobowych

GDPR General Data Protection Regulation

PROCES OCHRONY DANYCH OSOBOWYCH
PRAWA OSÓB KTÓRYCH DANE PRZETWARZAMY - PRZYKŁADY Z RODO

- Prawo do dostępu do zebranych danych osobowych
- Prawo do wiedzy i informacji o założeniach ewentualnego zautomatyzowanego przetwarzania danych
- Prawo do wiedzy i informacji o profilowaniu
- Prawo do wiedzy i informacji o konsekwencjach profilowania
- Prawo do wiedzy i informacji

PROCES OCHRONY DANYCH OSOBOWYCH
PRAWA OSÓB KTÓRYCH DANE PRZETWARZAMY - PRZYKŁADY Z RODO

- Prawo do udzielania zdalnego dostępu do bezpiecznego systemu zapewniającego bezpośredni dostęp do danych
- Prawo do nie naruszania tajemnicy handlowej, własności intelektualnej i praw autorskich
- Prawo do sprostowania danych
- Prawo do sprzeciwu co do przetwarzania danych osobowych
- Prawo do usunięcia danych (wewnątrz struktur administratora danych)

DANE OSOBOWE

UODO

Dane osobowe oznaczają **informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej** („osobie, której dane dotyczą”);

RODO

Wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (także wykonującej „osobową” działalność gospodarczą!), bez ponoszenia nadmiernych kosztów, czasu, działań w celu ustalenia tożsamości tej osoby

ROLE W RODO

„Administrator” - ustala cele i sposoby przetwarzania danych osobowych;

„Współadministrator” - co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania,

„Podmiot przetwarzający”(„procesor”) przetwarza dane osobowe w imieniu administratora;

PRZETWARZANIE DANYCH OSOBOWYCH

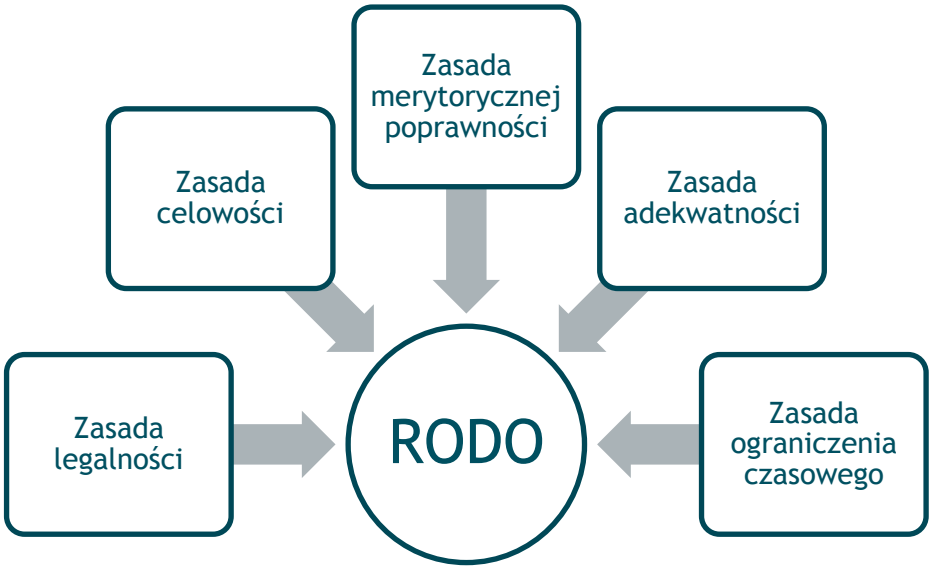
UODO

Przetwarzanie oznacza **operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych**

RODO

Jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;

JAK PRZETWARZAĆ DANE OSOBOWE ?



DLACZEGO PRZETWARZAĆ DANE OSOBOWE?

UODO (ART. 23)

Osoba wyraziła zgodę

Niezbędne do wykonania umowy,

Niezbędne do wypełnienia obowiązku prawnego;

Niezbędne do ochrony żywotnych interesów osoby;

Niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej

Niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora

RODO (ART. 61)

Osoba wyrazi na to zgodę;

Dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa;

Konieczne do realizacji umowy

Niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego;

Niezbędne dla prawnie usprawiedliwionych celów realizowanych przez administratorów danych

NOWE POJĘCIA W RODO

UODO

„pseudonimizacja” oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie,

RODO

„anonimizacja” zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

OBOWIĄZEK INFORMACYJNY – RODO (ART. 13-14)

Pozostał podział na obowiązki informacyjne w przypadku zbierania danych bezpośrednio od podmiotu danych oraz zbierania ich w inny sposób (inni administratorzy danych, dane ogólnodostępne)

Zachowano wyłączenie obowiązku informacyjnego, gdy podmiot danych dysponuje już tymi informacjami (art.13 ust.4 i art.14 ust.5a)

Rozszerzono zakres obowiązku informacyjnego w celu realizacji zasady przejrzystości (motyw nr 39 i 58):

- Adres i nazwa administratora danych,
- cel zbierania danych, odbiorcy lub ich kategorie
- prawo dostępu do treści danych oraz ich poprawiania;

OBOWIĄZEK INFORMACYJNY – RODO (ART. 13-14)

- dobrowolność albo obowiązek podania danych i jego podstawa prawna
- podstawa prawna przetwarzania,
- Informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję Europejską odpowiedniego stopnia ochrony
- okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu

ZADANIA ADMINISTRATORA DANYCH OSOBOWYCH
REJESTR CZYNNOŚCI PRZETWARZANIA

1. Każdy administrator oraz – gdy ma to zastosowanie –przedstawiciel administratora prowadzą rejestr czynności przetwarzania danych osobowych, za które odpowiadają.

- imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych;
- cele przetwarzania;
- opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;

ZADANIA ADMINISTRATORA DANYCH OSOBOWYCH
REJESTR CZYNNOŚCI PRZETWARZANIA

- kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
- gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń;
- jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
- jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.

ZADANIA ADMINISTRATORA DANYCH OSOBOWYCH
REJESTR KATEGORII CZYNNOŚCI PRZETWARZANIA

2. Każdy administrator oraz – gdy ma to zastosowanie –przedstawiciel administratora prowadzą rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora, zawierający następujące informacje:

- imię i nazwisko lub nazwa oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający, a gdy ma to zastosowanie – przedstawiciela administratora lub podmiotu przetwarzającego oraz inspektora ochrony danych;

ZADANIA ADMINISTRATORA DANYCH OSOBOWYCH
REJESTR KATEGORII CZYNNOŚCI PRZETWARZANIA

- kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;
- gdy ma to zastosowanie – przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń;
- jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.

ZADANIA ADMINISTRATORA DANYCH OSOBOWYCH
REJESTRY NIE ZAWSZE

Obowiązki, o których mowa w ust.1 i 2, nie mają zastosowania do przedsiębiorcy lub podmiotu zatrudniającego mniej niż 250 osób, chyba że

- przetwarzanie, którego dokonują, może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą,
- nie ma charakteru sporadycznego lub
- obejmuje szczególne kategorie danych osobowych, o których mowa w art.9 ust.1, lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa, o czym mowa w art.10.

Środki techniczno-organizacyjne dla zapewnienia poufności, integralności i rozliczalności danych osobowych

ODPOWIEDNIE ROZWIĄZANIA TECHNICZNE I ORGANIZACYJNE

Administrator danych powinien określić wykaz stosowanych w organizacji środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzania danych.

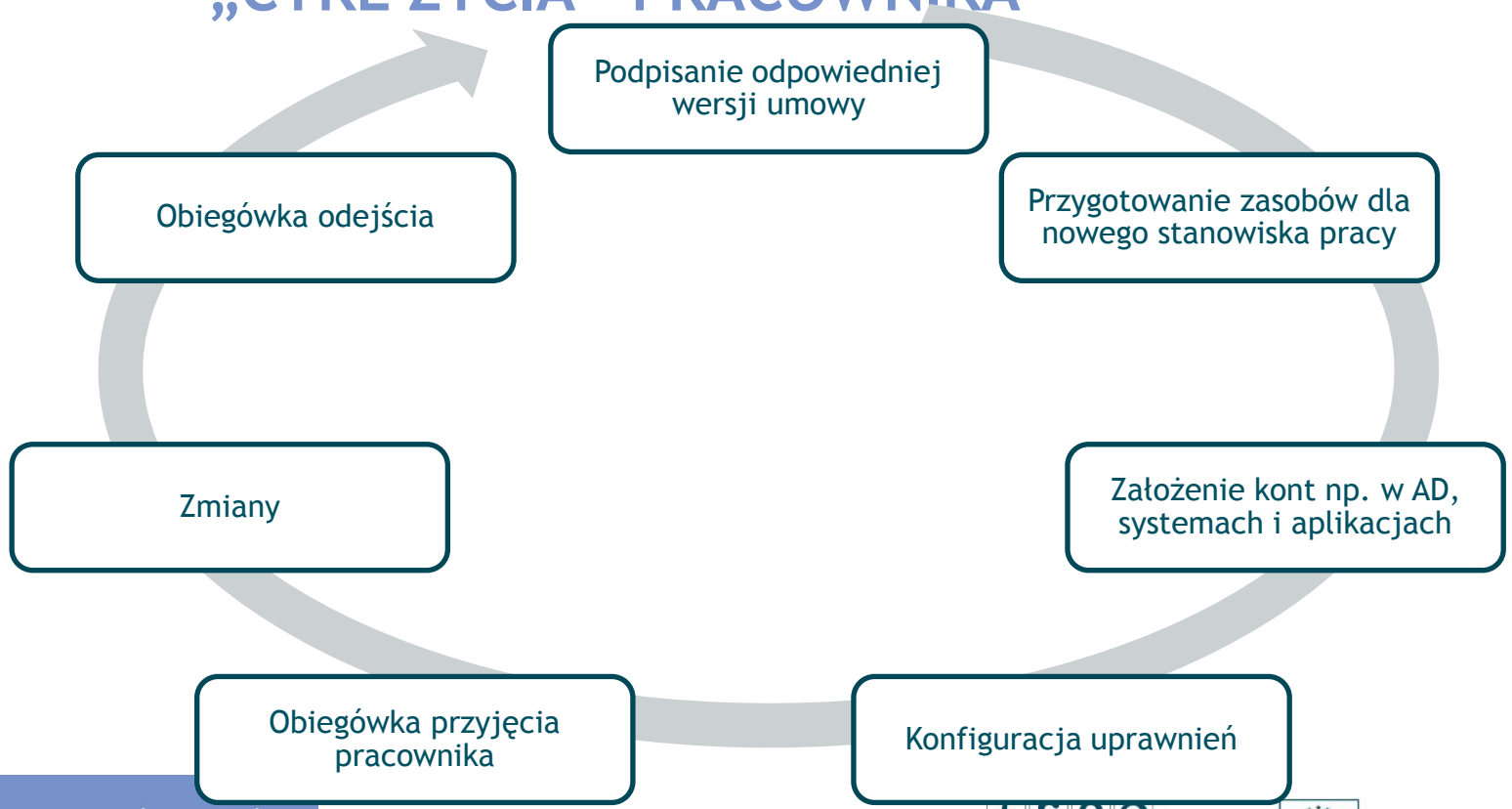
ZASADA ROZLICZALNOŚCI

System informatyczny zapewnia odnotowanie dla każdego rekordu:

- czasu wprowadzenia danych (data, godzina, minuta),
- źródła pochodzenia danych (pisemnie, adres IP, nr telefonu, …),
- nazwy użytkownika wprowadzającego dane,

Kadry i uczestnicy projektu

UMOWA Z PRACOWNIKIEM/WSPÓŁPRACOWNIKIEM
„CYKL ŻYCIA” PRACOWNIKA



ROZWIĄZANIE UMOWY

„CYKL ŻYCIA” DANYCH UŻYTKOWNIKA

- Usunięcie konta ≠ usunięcie danych
- Okresy przechowywania informacji
- Odmowa usunięcia danych
- Odmowa udostępnienia informacji

MAŁOLETNI W RODO

Trzeba odróżniać wyrażenie zgody na przekazanie danych osobowych od wyrażenia zgody na zawarcie umowy.

RODO nakazuje administratorowi podjęcie rozsądnych działań w celu weryfikacji zgody lub aprobaty rodzica lub opiekuna prawnego. Administrator może w tym celu na przykład wprowadzić zasadę uwierzytelniania przez inne konto, która pozwoli dziecku przesłać prośbę o zgodę do sprawdzonego konta rodzica na tym samym portalu.

MAŁOLETNI W RODO

Przykład: Uzyskiwanie zgody dziecka 10-letni Jaś chce wziąć udział w konkursie internetowym na najlepszy komiks. W formularzu zgłoszeniowym trzeba podać numer telefonu, można też wyrazić zgodę na cele marketingowe.

Czy organizatorzy mogą uzyskać zgodę Jasia na cele marketingowe?

MAŁOLETNI W RODO

Po pierwsze należy zaznaczyć, że do udziału Jasia w konkursie niezbędne będzie na gruncie prawa cywilnego wyrażenie zgody przez jego rodziców. Odnosząc się natomiast do wyrażenia przez Jasia zgody na cele marketingowe, to Jaś nie będzie mógł takiej zgody udzielić samodzielnie. Jaś musi o to poprosić rodzica bądź opiekuna prawnego. Jednak to na administratorze ciąży obowiązek podjęcia rozsądnych starań w celu zweryfikowania, czy osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem wyraziła zgodę lub ją zaaprobowała.

MAŁOLETNI W RODO

Dlatego organizatorzy konkursu powinni wyświetlić komunikat z zapytaniem o wiek. Natomiast po zaznaczeniu opcji wskazującej, że Jaś ma poniżej 16 lat (propozycja Ministra Cyfryzacji w nowym projekcie ustawy o ochronie danych osobowych obniża granicę do lat 13), powinien się wyświetlić następny komunikat, w którym zgodę na udział oraz na cele marketingowe może wyrazić tylko rodzic lub opiekun prawny.

Powierzenie przetwarzania danych osobowych

Art.31. Administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych.

POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

Administrator i inni w RODO

Administrator ma obowiązek korzystania wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą (art.28ust.1)

Podstawą przetwarzania ma być umowa, której treść została istotnie zmodyfikowana (art.28 ust.3 RODO) w stosunku do dotychczasowego stanu prawnego wynikającego z UODO, lub inny instrument prawny

POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

Treść umowy została istotnie zmodyfikowana w stosunku do dotychczasowego stanu prawnego (art.31 UODO vs. art.28 ust.3 RODO)

Procesor:

a) Przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora
b) Zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy;
c) Podejmuje wszelkie środki wymagane na mocy art.32
d) Przestrzega warunków korzystania z usług innego podmiotu przetwarzającego
e) Pomaga administratorowi
f) Po zakończeniu świadczenia usług usuwa lub zwraca mu wszelkie dane osobowe;
g) Udostępnia administratorowi wszelkie informacje oraz umożliwia administratorowi przeprowadzanie audytów, w tym inspekcji i przyczynia się do nich.

DO OBOWIĄZKÓW PROCESORA NALEŻY PROWADZENIE REJESTRU PRZETWARZANIA DANYCH

Administrator i procesor prowadzą, każdy we własnym zakresie, rejestry czynności przetwarzania

- Administrator prowadzi rejestr czynności przetwarzania danych osobowych, za które odpowiada
- Procesor prowadzi rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora

Każdy administrator lub podmiot przetwarzający udostępnia rejestr na żądanie organu nadzorczego

Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu

ZADANIA ADMINISTRATORA

Art.4 pkt 12 RODO

„naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych”

ZADANIA ADMINISTRATORA

Zgłaszanie naruszenia organowi nadzorczemu

W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza (art.33ust.1)

Zawiadomienia osób, których dane dotyczą:

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. (art.34ust.1)

Odpowiedzialność za naruszenie RODO

ODPOWIEDZIALNOŚĆ ZA NARUSZENIE PRZEPISÓW O OCHRONIE DANYCH OSOBOWYCH

Art.58 ust.2 Uprawnienia naprawcze Organu Nadzorczego

- Wydawanie ostrzeżeń
- Udzielanie upomnień
- Nakazanie spełnienia żądania osoby
- Nakazanie dostosowania operacji przetwarzania do przepisów

ODPOWIEDZIALNOŚĆ ZA NARUSZENIE PRZEPISÓW O OCHRONIE DANYCH OSOBOWYCH

Art.82 Prawo do odszkodowania i odpowiedzialność

1. Każda osoba która poniosła szkodę ma prawo uzyskać odszkodowanie

Art.83 Kary pieniężne

1. Na podmioty publiczne, o których mowa w art. 9 pkt 1 12 -i 14 UoFinPubl Prezes Urzędu może nałożyć, w drodze decyzji, administracyjne kary pieniężne w wysokości do 100 tyś zł. Nałożenie kary spowoduje odpowiedzialność urzędnika za dyscyplinę finansów publ.

Podsumowanie

PODSUMOWANIE ISTOTNYCH OBOWIĄZKÓW Z RODO

Organy i podmioty publiczne (zgodne z definicją formalną) mają obowiązek wyznaczenia Inspektora Ochrony Danych

Administracja musi działać ściśle według obowiązków i nakazów wynikających z przepisów prawa, w szczególności w zakresie techniczno-organizacyjnym obowiązuje ustawa o informatyzacji, rozporządzenie KRI i przepisy szczególne

Podstawą przetwarzania DO, co do zasady jest przepis prawa, nie ma dobrowolności typu „może coś przetwarzać”, skupia się tylko na „musi”

Nie ma możliwości korzystania z *prawnie uzasadnionego interesu*

PODSUMOWANIE ISTOTNYCH OBOWIĄZKÓW Z RODO

Administracja może korzystać ze zgody, w przypadku niestandardowych aktywności o charakterze publicznym (np. konkursy dla mieszkańców)

Brak jest swobody w określaniu celu i zakresu danych osobowych do przetwarzania (z wyj. Inicjatyw specjalnych)

Kara pieniężna została ograniczona do ustalonej w przepisach granicy, co jednak nie wyklucza roszczeń cywilnych ze strony poszkodowanych podmiotów

PODSUMOWANIE ISTOTNYCH OBOWIĄZKÓW Z RODO

Obowiązują zasady należytej staranności przy wyborze podwykonawców, procesorów, w szczególności w zakresie oceny ryzyka oraz obowiązku wyznaczenia u nich IOD

Przy konstruowaniu SIWZ publiczny zamawiający powinien wziąć pod uwagę powierzenie przetwarzania, określić, jakie warunki ma spełniać, żeby wykazać zgodność z art.28 ust.1