
OCHRONA DANYCH OSOBOWYCH W POMOCY SPOŁECZNEJ

Warszawa 15.10.2020 r.

Agenda

❑ **Informacje ogólne:**

- dane osobowe – wyjaśnienie pojęcia,
- kategorie danych,
- gdzie są przetwarzane dane,
- przetwarzanie danych osobowych – definicja,
- akty prawne dotyczące przetwarzania i ochrony danych osobowych obowiązujące do dnia 25.05.2018 r.,
- akty prawne dotyczące przetwarzania i ochrony danych osobowych obowiązujące od dnia 25.05.2018 r.,
- RODO w praktyce.

❑ **RODO - obowiązki Administratora:**

- RODO - obowiązki Administratora,
- RODO - obowiązki Administratora art. 32,
- Rozliczalność (typy ryzyka oraz sposoby jego szacowania, rejestry czynności oraz kategorii czynności, zasady oraz sposoby przeprowadzania DPIA),
- Omówienie technicznych oraz organizacyjnych środków ochrony.

Agenda

☐ **Kary:**

- ogólne warunki nakładania administracyjnych kar pieniężnych,
- RODO to nie fikcja – nałożone kary w Polsce,
- RODO to nie fikcja – przykładowe najwyższe kary w Europie.

☐ **Podstawy przetwarzania danych:**

- podstawy prawne do przetwarzania danych osobowych art. 6 RODO,
- podstawy prawne do przetwarzania danych osobowych art. 9 RODO,
- podstawy przetwarzania danych – monitoring.

☐ **Prawa osób, których dane dotyczą:**

- 10 wskazówek UODO, jak korzystać z praw gwarantowanych przez RODO,
- RODO - Prawa osób, których dane dotyczą.

☐ **Obowiązek informacyjny**

☐ **Role „stron” przetwarzania:**

- role „stron” przetwarzania - podstawy przetwarzania danych.

Agenda

☐ **Naruszenie czy incydent?:**

- naruszenie czy incydent? – art. 33 (naruszenia),
- obowiązki w zakresie zgłaszania naruszeń,
- zawiadamianie osoby, której dane dotyczą o naruszeniu ochrony danych osobowych – art. 34,

☐ **Zasady dotyczące przetwarzania danych osobowych**

- zasady przetwarzania danych w Ośrodku Pomocy Społecznej,
- ustawa o pomocy społecznej,
- ustawa o przeciwdziałaniu przemocy w rodzinie – zespół interdyscyplinarny oraz przetwarzanie danych w procedurze niebieskiej karty,

☐ **Warunki przetwarzania danych przez osoby upoważnione**

☐ **Inspektor ochrony danych:**

- zadania Inspektora Ochrony Danych.

Agenda

☐ **Kontrola UODO:**

- kontrola RODO – uprawnienia oraz zakres.

☐ **Podsumowanie:**

- 10 wskazówek UODO, jak stosować RODO,
- dobre praktyki w ochronie danych osobowych,
- korzystanie ze służbowej poczty e-mail,
- korzystanie ze służbowego komputera.

Informacje ogólne

Dane osobowe – wyjaśnienie pojęcia

- ❑ „Dane osobowe” oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
- ❑ Informacji nie uważa się za umożliwiającą określenie tożsamości, jeżeli wymagałoby to nadmiernych kosztów, czasu i działań.
- ❑ Danymi osobowymi nie są pojedyncze informacje o dużym stopniu ogólności, np. sama nazwa ulicy i numer domu.



Kategorie danych

- imię
- nazwisko
- adres zamieszkania
- PESEL
- NIP
- numer i seria dowodu osobistego
- wykształcenie
- zawód
- płeć
- numer telefonu

Dane zwykłe



- pochodzenie rasowe lub etniczne
- poglądy polityczne
- przekonania religijne lub światopoglądowe
- przynależność do związków zawodowych
- informacja o stanie zdrowia
- dane biometryczne, genetyczne
- seksualność
- orientacja seksualna

Art. 10 RODO

- wyroki skazujące
- czyny zabronione

Szczególna kategoria danych

(sensytywne, szczególnie chronione)



Gdzie są przetwarzane dane osobowe?

01

w kartotekach,
skorowidzach, księgach, wykazach
i w innych zbiorach ewidencyjnych

02

w systemach
informatycznych,
także w przypadku przetwarzania
danych poza zbiorem danych



Przetwarzanie danych osobowych

Operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.



Akty prawne dotyczące przetwarzania obowiązujące do dnia 25.05.2018 r.:

- ☐ **Konstytucja Rzeczypospolitej Polskiej.**
- ☐ Ustawa z dnia 29 sierpnia 1997 o Ochronie Danych
- ☐ **Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r.**
- ☐ **Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r.**

Akty prawne dotyczące przetwarzania obowiązujące od dnia 25.05.2018 r.:

- ☐ ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r.
- ☐ DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/680 z dnia 27 kwietnia 2016 r..
- ☐ Ustawa z dnia 10 maja 2018 r. O Ochronie Danych Osobowych.
- ☐ Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania RODO.



RODO w praktyce

- ☐ RODO ma bezpośrednie oddziaływanie i nie wymaga implementacji do porządku prawnego RP.
- ☐ Dzięki RODO wzrasta waga ochrony danych osobowych.
- ☐ RODO nie wymaga uchwalenia przepisów transponujących.
- ☐ Od 25.05.2018 r. spadkobiercą GIODO stanie się UODO.
- ☐ Rozszerzenie pojęcia danych osobowych.
- ☐ **Podejście oparte na ryzyku.**
- ☐ Obligatoryjne w wielu przypadkach – **powołanie IOD.**
- ☐ Wysokie kary pieniężne.
- ☐ Nowy obowiązek informacyjny.
- ☐ Nowe pojęcia dotyczące: ograniczenie przetwarzania, profilowanie, pseudonimizacja, anonimizacja.



RODO - obowiązki Administratora

RODO – obowiązki Administratora

- ☐ Art. 35 RODO – przeprowadzenie Oceny Skutków dla ochrony danych.
- ☐ Art. 30 RODO – prowadzenie rejestru czynności przetwarzania.
- ☐ Wdrożenie polityk ochrony danych.
- ☐ Stosowanie zasady, zgodnie z art. 25 ust. 1 (*privacy by design*).
- ☐ Stosowanie zasady *privacy by default*, (art. 25 ust. 2. RODO)
- ☐ Notyfikacja naruszeń związanych z ochroną danych do organu w ciągu 72 h.
- ☐ Wprowadzenie nowych klauzul do dokumentacji, umów wg nowych wytycznych.
- ☐ Realizacja nowych praw osoby, której dane dotyczą.
- ☐ Jeżeli przetwarzanie odbywa się na podstawie zgody to na ADO spoczywać będzie obowiązek wykazania, że osoba której dane dotyczą wyraziła zgodę na przetwarzanie.



RODO – obowiązki Administratora - art. 32

- ☐ Wdrożenie adekwatnych środków technicznych i organizacyjnych.
- ☐ Zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania.
- ☐ Zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich.
- ☐ Regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych.
- ☐ Ocena, czy stopień bezpieczeństwa jest odpowiedni w oparciu o ryzyko przetwarzania.



Rozliczalność

- ☐ Szacowanie ryzyka a zakres wdrożonej dokumentacji oraz środków – metodyka.
- ☐ Udokumentowanie wdrożenia adekwatnych środków technicznych i organizacyjnych.
- ☐ Dokumentowanie procesów przetwarzania – rejestry czynności oraz rejestry kategorii czynności.
- ☐ Polityki ochrony danych.
- ☐ Prowadzenie rejestrów umów powierzenia oraz udostępnień danych osobowych.
- ☐ Stworzenie odpowiednich procedur realizacji praw osób, których dane dotyczą.

Omówienie technicznych oraz organizacyjnych środków ochrony

- ☐ Środki ochrony fizycznej danych.
- ☐ Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej.
- ☐ Środki ochrony w ramach narzędzi programowych i baz danych.
- ☐ Środki organizacyjne.



Kary

Ogólne warunki nakładania administracyjnych kar pieniężnych

- ❑ Kary skuteczne, proporcjonalne i odstraszające.
- ❑ Decydując, czy nałożyć karę pieniężną, zwraca się należytą uwagę na:
 - charakter, wagę i czas trwania naruszenia,
 - umyślny lub nieumyślny charakter naruszenia,
 - działania podjęte w celu zminimalizowania szkody,
 - stopień odpowiedzialności administratora lub podmiotu przetwarzającego,
 - wszelkie stosowane wcześniej naruszenia,
 - stopień współpracy z organem nadzorczym,
 - kategorie danych osobowych, których dotyczyło naruszenie,
 - sposób, w jaki organ nadzorczy dowiedział się o naruszeniu.



RODO to nie fikcja – nałożone kary w Polsce

Lp	Kwota (PLN)	Kwota (EUR)	Data	Nazwa i określenie podmiotu	Powód
1	50 000,00	11 682,24	10.09.2020	SGGW w Warszawie	Naruszenie - kradzież laptopa z danymi
2	100 000,00	23 364,49	02.09.2020	Główny Geodeta Kraju z siedzibą w Warszawie	Brak współpracy z UODO oraz niedostosowanie się do decyzji UODO
3	5 000,00	1 168,22	03.06.2020	Niepubliczny żłobek i przedszkole	Brak współpracy z UODO w związku z naruszeniem
4	15 000,00	3 504,67	29.05.2020	East Power sp. z o.o.	Brak współpracy z UODO
5	20 000,00	4 672,00	09.03.2020	Vis Consulting sp. z o.o.	Brak współpracy z UODO
6	2 830 410,00	660 000,00	10.09.2019	MoreleNet Sp. z o.o.	Naruszenie - niewystarczające zabezpieczenia systemów informatycznych (atak hakerski)
7	55 750,50	13 000,00	25.04.2019	Dolnośląski Związek Piłki Nożnej	Naruszenie - upublicznienie peseli i miejsca zamieszkania sędziów
8	943 470,00	220 000,00	15.03.2019	Bisnode Sp. z o.o.	Naruszenie
9	201 559,50	47 000,00	16.10.2019	ClickQuickNow	Naruszenie - lekceważenie prawa do wycofania zgody na przetwarzanie danych osobowych oraz prawa do bycia zapomnianym
10	40 000,00	9 400,00	18.10.2019	Burmistrz Aleksandrowa Kujawskiego	Brak kopii zapasowych transmisji obrad sesji, brak umowy powierzenia, brak współpracy z UODO
11	20 000,00	4 784,69	2019	Szkoła Podstawowa w Gdańsku	Przetwarzanie danych nadmiarowych dzieci (linie papilarne przy wejściu do stołówki)
12	1 973,00	460,00	2019	Wspólnota mieszkaniowa	Naruszenie
13	8 148,00	1 900,00	2019	Spółka Zarządzająca Nieruchomościami	Naruszenie
14	30 019,50	7 000,00	2019	Spółka zajmująca się ochroną mienia i ludzi	Naruszenie



RODO to nie fikcja – przykładowe najwyższe kary w Europie

- ❑ Wind Tre we Włoszech – 16,7 mln EUR.**
- ❑ Poczta Austriacka – 18 mln EUR.**
- ❑ TIM (operator telekomunikacyjny) we Włoszech – 27,8 mln EUR.**
- ❑ Google we Francji – 50 mln EUR.**
- ❑ Hotele Marriott w UK – 110,4 mln EUR.**
- ❑ British Airways – 204,6 mln EUR.**



Podstawy przetwarzania danych

Podstawy prawne do przetwarzania danych osobowych art. 6 RODO

- ☐ Osoba, której dane dotyczą wyraziła zgodę na przetwarzanie – art. 6 ust. 1 lit a.
- ☐ Przetwarzanie jest niezbędne do wykonania umowy – art. 6 ust. 1 lit b
- ☐ Przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze – art. 6 ust. 1 lit c.
- ☐ Przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej – art. 6 ust. 1 lit d.
- ☐ Przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi – art. 6 ust. 1 lit e.
- ☐ Przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora. Akapit pierwszy lit. f) nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań. 2. – art. 6 ust. 1 lit f.



Podstawy prawne do przetwarzania danych osobowych art. 9 RODO

- ☐ Osoba, której dane dotyczą wyraziła zgodę na przetwarzanie – art. 9 ust. 2 lit a.
- ☐ Przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej – art. 9 ust. 2 lit b.
- ☐ Przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej – art. 9 ust. 2 lit c.
- ☐ Przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych – art. 9 ust. 2 lit d.
- ☐ Przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą – art. 9 ust. 2 lit e



Podstawy prawne do przetwarzania danych osobowych art. 9 RODO – cd.

- ☐ Przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń – art. 9 ust. 2 lit f.
- ☐ Przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego – art. 9 ust. 2 lit g.
- ☐ Przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego – art. 9 ust. 2 lit h.
- ☐ przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi – art. 9 ust. 2 lit i.
- ☐ Przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 – art. 9 ust. 2 lit j.



Podstawy przetwarzania danych - monitoring

❑ Zasady przetwarzania danych:

- podstawa prawna,
- okres retencji,
- zmiany w nowelizacji RODO.

❑ Zasady udostępniania nagrań z monitoringu:

- udostępnienie wnioskodawcy,
- ograniczenie przetwarzania,
- ograniczenie przetwarzania -> PUODO.



Prawa osób, których dane dotyczą

10 wskazówek UODO jak korzystać z praw gwarantowanych przez RODO

- ☐ Każdy ma prawo wiedzieć, co będzie się działo z jego danymi.
- ☐ Każdy ma prawo w każdej chwili wycofać zgodę.
- ☐ Informacja o przetwarzaniu danych powinna być przekazywana w sposób jasny i zrozumiały.
- ☐ Nie ze wszystkich praw osoba, której dane dotyczą może skorzystać.
- ☐ Każda osoba, której dane dotyczą ma prawo do informacji o naruszeniu jej danych.
- ☐ Jeżeli zostanie wniesiony sprzeciw - marketing nie może być prowadzony.
- ☐ Należy chronić dzieci przed nieuczciwymi praktykami.
- ☐ Osoba, której dane dotyczą, najpierw powinna żądać od administratora realizacji praw.
- ☐ Każda osoba, której dane dotyczą może dochodzić swoich praw przed sądem.
- ☐ Każda osoba ma prawo złożyć skargę do UODO.



RODO - Prawa osób, których dane dotyczą

☐ Prawo dostępu:

- prawo do informacji o przetwarzaniu danych,
- prawo do kopii danych.

☐ Prawo do sprostowania.

☐ Prawo do usunięcia (prawo do bycia zapomnianym).

☐ Prawo do ograniczenia przetwarzania.

☐ Prawo do przenoszenia (art. 6 ust. 1 lit a, b; art. 9 ust. 2 lit a).

☐ Prawo sprzeciwu (art. 6 ust. 1 lit e, f; marketing bezpośredni).

☐ Prawo wniesienia skargi do Urzędu Ochrony Danych.

☐ Art. 82 RODO - żądanie odszkodowania od ADO.



RODO - Prawa osób, których dane dotyczą – cd.

- ❑ Bezpłatny dostęp do danych osobowych.
- ❑ Miesiąc na odpowiedź: (realizacja żądania, odmowa realizacji, żądania, informacja o przedłużeniu realizacji żądania, powtarzające się żądania).
- ❑ Przejrzystość – Art. 12.
- ❑ Zależności pomiędzy prawami osób których dane dotyczą a podstawami przetwarzania danych osobowych:
 - przetwarzanie na podstawie zgody, a prawa osób,
 - przetwarzanie na podstawie umowy, a prawa osób,
 - przetwarzanie na podstawie obowiązku prawnego, a prawa osób,
 - przetwarzanie na podstawie interesu publicznego, a prawa osób,
 - przetwarzanie na podstawie uzasadnionego interesu a prawa osób,
 - test równowagi.



Obowiązek informacyjny

RODO – Obowiązek informacyjny



- ☐ Zbieranie danych od osoby, której dane dotyczą – art. 13 RODO.
- ☐ Zbieranie danych z innych źródeł – art. 14.
- ☐ **Warstwowe spełnianie obowiązku informacyjnego (EROD):**
 - nazwa i dane kontaktowe administratora,
 - cel i podstawy przetwarzania,
 - prawa osób, których dane dotyczą,
 - odesłanie do pełnego obowiązku, np. na stronie www.
- ☐ **Ograniczenia obowiązku z art. 13**
 - jedynie gdy i w zakresie, w jakim osoba, dysponuje już tymi informacjami
- ☐ **Ograniczenia obowiązku z art. 14:**
 - osoba, której dane dotyczą, dysponuje już tymi informacjami,
 - udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku,
 - pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem,
 - dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy.

RODO – Obowiązek informacyjny

Art. 24 UODO

- ✓ Adres siedziby i pełna nazwa
- ✓ Cel zbierania danych
- ✓ Odbiorcy lub kategorie odbiorców
- ✓ Prawo dostępu do treści swoich danych oraz ich poprawiania
- ✓ Informacja o dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej



Art. 13 RODO

- ✓ Tożsamość administratora i dane kontaktowe
- ✓ Dane kontaktowe IOD
- ✓ Cel przetwarzania i **podstawa prawna**
- ✓ **Prawnie uzasadniony interes**
- ✓ Odbiorcy danych lub kategorie odbiorców
- ✓ **Przekazanie danych do państwa trzeciego**
- ✓ **Okres przechowywania**
- ✓ Prawa osób
- ✓ Odwołanie zgody
- ✓ **Prawo do złożenia skargi**
- ✓ Informacja o obowiązku lub dobrowolności podania danych i konsekwencjach niepodania danych
- ✓ **Zautomatyzowane podejmowanie decyzji**

RODO – Obowiązek informacyjny

Art. 25 UODO

- ✓ Adres siedziby i pełna nazwa
- ✓ Cel zbierania danych
- ✓ Zakres danych
- ✓ Odbiorcy lub kategorie odbiorców
- ✓ Źródło danych
- ✓ Prawo dostępu do treści swoich danych oraz ich poprawiania
- ✓ Prawo sprzeciwu



Art. 14 RODO

- ✓ Tożsamość administratora i dane kontaktowe
- ✓ Dane kontaktowe IOD
- ✓ Cel przetwarzania i **podstawa prawna**
- ✓ **Prawnie uzasadniony interes**
- ✓ Odbiorcy danych lub kategorie odbiorców
- ✓ Kategorie danych
- ✓ **Przekazanie danych do państwa trzeciego**
- ✓ **Okres przechowywania**
- ✓ Źródło danych
- ✓ Prawa osób
- ✓ **Odwołanie zgody**
- ✓ **Prawo do złożenia skargi**
- ✓ **Zautomatyzowane podejmowanie decyzji**

RODO – Obowiązek informacyjny

- ☐ **Doprecyzowanie celów przetwarzania danych osobowych w klauzuli informacyjnej, aby uwzględniała przetwarzanie danych w przyszłych procesach.**
- ☐ **Dopuszczalne formy spełnienia obowiązku informacyjnego:**
 - pisemna,
 - elektroniczna,
 - ustna, na życzenie osoby,
 - warstwowa.

Najczęściej popełniane błędy:

- nieprawidłowo wskazany administrator danych,
- nieprawidłowy katalog aktów prawnych,
- umieszczanie w katalogu aktów prawnych niebędących aktami prawnymi,
- wskazywanie zgody osoby, w przypadku kiedy podstawą przetwarzania nie jest zgoda,
- niedopasowanie katalogu praw przysługujących podmiotowi.



Role „stron” przetwarzania

Role „stron” przetwarzania

- ☐ Administrator.
- ☐ Podmiot przetwarzający.
- ☐ Odbiorca.
- ☐ Współadministrator.
- ☐ Kiedy powinna być zawarta umowa powierzenia danych – art. 28?
 - umowa powierzenia - lista kontrolna,
 - przykładowa umowa powierzenia danych,
 - ankieta zgodności z RODO dla podmiotu przetwarzającego.
- ☐ Kiedy powinna być zawarta umowa udostępnienia danych?
 - porozumienie w przedmiocie przetwarzania danych.



Role „stron” przetwarzania

- ☐ Przetwarzanie na podstawie upoważnienia oraz oświadczenia o zachowaniu poufności.
- ☐ Upoważnienie do przetwarzania danych przed i po nowelizacji RODO.
- ☐ Upoważnienia do przetwarzania danych a obowiązki służbowe – kiedy dodatkowe upoważnienia?
- ☐ Zakres zbieranych danych przed i po nowelizacji RODO.
- ☐ Dane nadmiarowe.
- ☐ Minimalizacja.



Naruszenie czy incydent?

Naruszenie czy incydent? – art. 33

- ❑ Naruszenie czy incydent?
- ❑ Kiedy mamy do czynienia z naruszeniem?
 - naruszenie poufności,
 - naruszenie dostępności,
 - naruszenie integralności.



Obowiązki w zakresie zgłaszania naruszeń

- ☐ 72 godziny na zgłoszenie naruszenia - art. 55.
- ☐ Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi. **Informacja o naruszeniu powinna:**
 - 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,
 - zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych,
 - opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,
 - opisywać zastosowane środki zaradcze,
 - dodatkowe informacje umożliwiające ocenę ryzyka.
- ☐ Kiedy należy poinformować osobę której dane dotyczą o naruszeniu (art. 34)?



Zasady dotyczące przetwarzania danych osobowych

Zasady dotyczące przetwarzania danych osobowych

Dane osobowe muszą być:

- przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą,
- zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami,
- adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”),
- prawidłowe i w razie potrzeby uaktualniane,
- przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, **przez okres nie dłuższy, niż jest to niezbędne do celów**, w których dane te są przetwarzane,
- przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych.



Zasady dotyczące przetwarzania danych osobowych – cd.

- ☐ Zabronione jest automatyczne zaznaczanie zgody – zgoda musi być dobrowolna, konkretna oraz świadoma.
- ☐ Zakaz łączenia zgód na przetwarzanie danych (np. zgoda na przetwarzanie danych w celach marketingowych ze zgodą na przesyłanie drogą elektroniczną).
- ☐ Klauzula zgody musi być jasna i przejrzysta, zgoda musi dotyczyć konkretnego celu.
- ☐ Odrębna zgoda dla każdego celu przetwarzania.
- ☐ Zgoda musi być wyrażona bez przymusu.
- ☐ Przetwarzanie danych osobowych dzieci do 16 r. życia.



Zasady dotyczące przetwarzania danych osobowych – cd.

☐ Zgoda osoby, której dane dotyczą:

- okazanie woli – dane zwykłe – CV,
- działanie dobrowolne, konkretne, świadome i jednoznaczne – dane zwykłe,
- w formie oświadczenia lub wyraźnego działania potwierdzającego – dane szczególnej kategorii oraz profilowanie.



Zasady przetwarzania danych w ośrodku pomocy społecznej

- ☐ Kto jest administratorem danych osobowych? - Jednostki organizacyjne pomocy społecznej jako ADO – doprecyzowanie administratora.
- ☐ Pisemne upoważnienie do przetwarzania danych osobowych oraz oświadczenie o zachowaniu w poufności osób przetwarzających dane w imieniu OPS.
- ☐ Wzajemne udostępnianie danych pomiędzy jednostkami sektora finansów publicznych, sądy, policja, ZUS, KRUS i organy administracji publicznej, kuratorzy sądowi, pracodawcy, podmioty wykonujące działalność leczniczą, przedszkola, szkoły, placówki, poradnie i ośrodki, szkoły wyższe, organizacje pozarządowe są zobowiązani niezwłocznie, nie później jednak niż w terminie 7 dni od dnia otrzymania wniosku kierownika ośrodka pomocy społecznej, dyrektora centrum usług społecznych lub pracownika socjalnego udostępnić informacje, które mają znaczenie dla rozstrzygnięcia o przyznaniu lub wysokości świadczeń z pomocy społecznej, dla ustalenia wysokości odpłatności za świadczenia z pomocy społecznej lub dla weryfikacji uprawnień do świadczeń z pomocy społecznej.



Zasady przetwarzania danych w ośrodku pomocy społecznej –cd.

☐ KPA – Kodeks postępowania administracyjnego:

- spełnienie obowiązku informacyjnego przy pierwszej czynności skierowanej do strony, chyba że strona posiada te informacje, a ich zakres lub treść nie uległy zmianie,
- spełnienie obowiązku informacyjnego przy przekazaniu sprawy w zakresie danych przetwarzanych przez organ przekazujący,
- wgląd w akta sprawy następuje z pominięciem danych osobowych osoby składającej skargę, chyba że osoba skarżąca wyrazi na to zgodę,
- prawo dostępu do danych – bez dostępu do danych osoby składającej skargę,
- w sprawach załatwianych milcząco organ administracji publicznej udostępnia informacje, o których mowa w art. 13 ust. 1 i 2 rozporządzenia 2016/679, **w Biuletynie Informacji Publicznej na swojej stronie podmiotowej, na swojej stronie internetowej oraz w widocznym miejscu w swojej siedzibie oraz dodatkowo przy pierwszej czynności skierowanej do strony.**



Zasady przetwarzania danych w ośrodku pomocy społecznej –cd.

☐ Obowiązek należy również spełnić przy:

- wydawaniu zaświadczeń,
- przyjmowaniu i rozpatrywaniu skarg i wniosków,
- przekazywaniu skargi do organu właściwego.



Ustawa o pomocy społecznej

- ❑ Ustawa z dnia 12 marca 2004 r. o pomocy społecznej (art. 100) - OPS może przetwarzać dane członków rodzin.
- ❑ Dostęp do danych w rejestrze centralnym mają:
 - ośrodek pomocy społecznej oraz powiatowe centrum pomocy rodzinie,
 - wojewoda w stosunku do osób, które uzyskały w Rzeczypospolitej Polskiej status uchodźcy, ochronę uzupełniającą lub zezwolenie na pobyt czasowy,
 - organ właściwy, o którym mowa w art. 3 pkt 11 ustawy z dnia 28 listopada 2003 r. o świadczeniach rodzinnych (wójt, burmistrz, prezydent).
- ❑ Okres przechowywania - 10 lat licząc od dnia zaprzestania świadczeń - dla osób, którym odmówiono wsparcia - 1 rok.



Ustawa o pomocy społecznej – cd.

- ☐ W związku z przetwarzaniem danych osobowych w celu udzielenia świadczeń: udzielenie świadczeń w postaci interwencji kryzysowej, pracy socjalnej, poradnictwa, uczestnictwa w zajęciach klubu samopomocy, klubu samopomocy dla osób z zaburzeniami psychicznymi, schronienia w formie ogrzewalni i noclegowni, sprawienia pogrzebu, a także przyznanie biletu kredytowanego oraz w celu świadczenia usług w ośrodkach wsparcia, rodzinnych domach pomocy, mieszkaniach chronionych i domach pomocy społecznej; wykonanie obowiązku, o którym mowa w art. 13 ust. 1 i 2 RODO, następuje przez zamieszczenie informacji, o których mowa w art. 13 ust. 1 i 2 tego rozporządzenia, w widocznym miejscu w budynku, w którym udzielane są świadczenia lub świadczone usługi.
- ☐ Administrator danych informuje o powyższym ograniczeniu najpóźniej przy pierwszej czynności skierowanej do osoby, której dane dotyczą.



Ustawa o przeciwdziałaniu przemocy w rodzinie – zespół interdyscyplinarny oraz przetwarzanie danych w procedurze niebieskiej karty

- ☐ Ustawa z dnia 29 lipca 2005 r. o przeciwdziałaniu przemocy w rodzinie (art. 9c) – podejrzani/sprawcy przemocy nie mają dostępu do dokumentacji zawierającej dane osób dotkniętych przemocą lub osób zgłaszających – doprecyzowanie zakresu zbieranych danych.
- ☐ Zespół interdyscyplinarny powołuje wójt, burmistrz albo prezydent miasta – art. 9a.
- ☐ Obsługę organizacyjno-techniczną zespołu interdyscyplinarnego zapewnia ośrodek pomocy społecznej.
- ☐ Art. 9c pkt 3 informacja o konieczności podpisania oświadczenia o zachowaniu w poufności, które wydaje organ powołujący, czyli wójt, burmistrz albo prezydent miasta.
- ☐ Art. 9c pkt 6 Administratorem danych przetwarzanych na podstawie przepisów niniejszego artykułu jest ośrodek pomocy społecznej zapewniający obsługę organizacyjno-techniczną zespołu interdyscyplinarnego.
- ☐ Art. 9c pkt. 7 tego samego artykułu jest natomiast wskazanie obowiązków ciążących na administratorze w zakresie wydania upoważnienia do przetwarzania danych członkom zespołu i grup oraz oświadczenia o zachowaniu w tajemnicy

Ustawa o przeciwdziałaniu przemocy w rodzinie – cd.

- ❑ Osoby (**podejrzani /sprawcy przemocy**), mają dostęp do dokumentacji, z wyłączeniem dostępu do dokumentacji zawierającej dane osób dotkniętych przemocą w rodzinie oraz osób zgłaszających podejrzenie stosowania przemocy w rodzinie, których udostępnienie mogłoby spowodować zagrożenie życia, zdrowia lub bezpieczeństwa osób dotkniętych przemocą w rodzinie lub osób zgłaszających podejrzenie stosowania przemocy w rodzinie, w szczególności z wyłączeniem dostępu do:
- formularzy „Niebieska Karta” zawierających dane osób dotkniętych przemocą w rodzinie,
 - protokołów z posiedzeń zespołu interdyscyplinarnego oraz grup roboczych, chyba, że dotyczą wyłącznie działań podejmowanych wobec osób, co do których istnieje podejrzenie, że stosują przemoc w rodzinie oraz osób stosujących przemoc w rodzinie,



Ustawa o przeciwdziałaniu przemocy w rodzinie - cd

- notatek i dokumentów wytworzonych przy realizacji zadań, chyba że dokumenty te dotyczą wyłącznie działań podejmowanych wobec osób, co do których istnieje podejrzenie, że stosują przemoc w rodzinie oraz osób stosujących przemoc w rodzinie,
 - innych dokumentów zgromadzonych przy realizacji zadań, których udostępnienie mogłoby spowodować zagrożenie życia, zdrowia lub bezpieczeństwa osób dotkniętych przemocą w rodzinie lub osób zgłaszających podejrzenie stosowania przemocy w rodzinie.
- ☐ Podejmowanie interwencji w środowisku wobec rodziny dotkniętej przemocą odbywa się w oparciu o procedurę „Niebieskie Karty” i nie wymaga zgody osoby dotkniętej przemocą w rodzinie.



**Warunki przewarżania danych przez osoby
upoważnione**

Warunki przetwarzania danych osobowych

Pracownik może przetwarzać dane, tylko i wyłącznie w sytuacji, gdy:

- ☐ Zapoznał się z przepisami dotyczącymi ochrony danych osobowych, w tym z procedurami instrukcjami wprowadzonymi do stosowania przez zarządzenie
 - regulamin służbowej poczty email,
 - regulamin użytkowania komputera służbowego,
 - politykami ochrony danych osobowych.
- ☐ Posiada pisemne **upoważnienie** do przetwarzania danych osobowych
 - upoważnienie do przetwarzania danych - przykład
- ☐ Jest umieszczony w **Ewidencji Osób Upoważnionych** do przetwarzania danych:
 - z **określeniem celu i zakresu** wskazanym w upoważnieniu,
 - przez **okres** na jaki upoważnienie zostało udzielone.



Inspektor ochrony danych

Zapewnienie odpowiednich środków ochrony (technicznych i organizacyjnych) – Inspektor Ochrony Danych (IOD)

Obowiązek powołania

- ☐ Przetwarzania dokonują organ lub podmiot publiczny.
- ☐ Główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę.
- ☐ Główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10.



RODO – Inspektor Ochrony Danych IOD

- ☐ Z obsługi jednego IOD może korzystać wielu ADO.
- ☐ Wyznaczenie jednego IOD dla kilku podmiotów.
- ☐ Art. 37 ust. 6 RODO - Inspektor Ochrony Danych może być członkiem personelu administratora lub wykonywać zadania na podstawie umowy o świadczenie usług.
- ☐ Art. 37 ust 5 RODO - Inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej.
- ☐ Administrator lub podmiot przetwarzający publikują dane kontaktowe inspektora ochrony danych i zawiadamiają o nich organ nadzorczy.
- ☐ ADO i podmiot przetwarzający zostali zobowiązani do zapewnienia Inspektorowi zasobów niezbędnych do utrzymania jego wiedzy fachowej.
- ☐ IOD – gwarancja niezależności i unikanie konfliktu interesów motyw 97 RODO.
- ☐ IOD musi być włączany we wszystkie sprawy dotyczące ochrony danych.



Zadania Inspektora Ochrony Danych

- ☐ Art. 39.1.a – informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO.
- ☐ Art. 39.1.b monitorowanie przestrzegania niniejszego rozporządzenia, działania zwiększające świadomość, szkolenia personelu oraz powiązane z tym audyty.
- ☐ Art. 39.1.c udzielanie na żądanie zaleceń, co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35.
- ☐ Art. 39.1.d współpraca z organem nadzorczym.
- ☐ Art. 39.1.e pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem.
- ☐ Pełnienie punktu kontaktowego dla osób, których dane dotyczą.
- ☐ Prowadzenie rejestru czynności i rejestru kategorii czynności – zgodnie z art. 30
- ☐ Funkcja Zastępcy Inspektora Ochrony Danych
 - wymagania,
 - zgłoszenie do PUODO.



Kontrola UODO

Kontrola UODO – uprawnienia oraz zakres

UODO ma prawo do:

- ☐ Wstępu, w godzinach pracy podmiotu kontrolowanego, za okazaniem imiennego upoważnienia, do pomieszczeń, w których znajduje się zbiór powierzonych do przetwarzania danych osobowych oraz pomieszczeń, w których powierzone do przetwarzania dane osobowe są przetwarzane poza zbiorem danych osobowych.
- ☐ Żądania złożenia pisemnych lub ustnych wyjaśnień przez osoby upoważnione do przetwarzania powierzonych do przetwarzania danych osobowych oraz przez pracowników Instytucji Wdrażającej w zakresie niezbędnym do ustalenia stanu faktycznego.
- ☐ Wglądu do wszelkich dokumentów mających bezpośredni związek z przedmiotem kontroli lub audytu oraz sporządzania ich kopii.
- ☐ Przeprowadzania oględzin urządzeń, nośników oraz systemu informatycznego służącego do przetwarzania powierzonych do przetwarzania danych osobowych.



Podsumowanie

10 wskazówek UODO, jak stosować RODO

- ☐ Ustal właściwą podstawę zbierania i wykorzystywania danych osobowych.
- ☐ Dopełniaj obowiązku informacyjnego zgodnie z nowymi zasadami.
- ☐ Komunikuj się w sposób przejrzysty.
- ☐ W każdej sytuacji dbaj o respektowanie praw osób.
- ☐ Pamiętaj, że zgoda może być wycofana w każdym momencie.
- ☐ Naruszenia ochrony danych zgłaszaj do Prezesa UODO, a gdy trzeba informuj o nich również osoby, których dane zostały naruszone.
- ☐ Nie twórz niepotrzebnej dokumentacji.
- ☐ Masz prawo profilować, ale pamiętaj o ograniczeniach.
- ☐ Zainwestuj w fachowego IOD.
- ☐ Uważaj na oszustów.

<https://uodo.gov.pl/pl/171/578>



Dobre praktyki w ochronie danych osobowych

- ☐ Za bezpieczeństwo przetwarzania danych osobowych odpowiedzialność ponosi każdy pracownik mający dostęp i upoważnienie do danych osobowych.
- ☐ Pracownicy mający dostęp do danych osobowych nie mogą ich ujawniać zarówno w miejscu pracy, jak i poza nim.
- ☐ **Zawsze przy opuszczaniu stanowiska pracy (nawet na chwilę) pamiętaj o zabezpieczeniu dokumentów oraz komputera.**
- ☐ **Bądź ostrożny i świadomy otoczenia, gdy omawiasz sprawy poufne.**
- ☐ Nie wolno **przekazywać danych w żadnej formie** (elektronicznej, papierowej) **osobom trzecim**, które nie są uprawnione do dostępu do nich.
- ☐ **Nie wolno udzielać informacji, w których podawane są dane osobowe w formie zapytania telefonicznego bez uprzedniej weryfikacji osoby.**
- ☐ Wszystkie zbędne dane w formie kopii muszą zostać niezwłocznie zniszczone w sposób uniemożliwiający ich odczytanie.



Dobre praktyki w ochronie danych osobowych c.d.

- ☐ Przebywanie osób nieuprawnionych w pomieszczeniu, w którym przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych, chyba że dane te są w odpowiedni sposób zabezpieczone przed dostępem.
- ☐ Ujawnianie przez użytkownika osobie trzeciej haseł tymczasowych, haseł osobistych lub innych haseł mu powierzonych jest zabronione.
- ☐ Nie wolno prosić osoby, której dane dotyczą o podanie danych osobowych, które wykraczają poza zakres niezbędny do wykonania zamierzonego celu.
- ☐ Zabrania się wykorzystywania danych osobowych w celach innych niż te, do których zostały zebrane i na które osoba zainteresowana wyraziła zgodę.



KORZYSTANIE ZE SŁUŻBOWEJ POCZTY E-MAIL

- ☐ Zabrania się przesyłania przez pracownika dokumentów firmowych na swoje prywatne adresy e-mail.
- ☐ **Niezaszyfrowana poczta e-mail może służyć wyłącznie do przesyłania dokumentów, które nie zawierają danych osobowych, danych wrażliwych czy poufnych.**
- ☐ Nie wolno przysyłać niezaszyfrowaną pocztą e-mail **żadnych** danych osobowych klientów oraz pracowników, informacji o wysokości wynagrodzenia itp.
- ☐ Nie wolno prosić o przesłanie danych osobowych lub innych danych wrażliwych e-mailem, należy poprosić ewentualnie o dostarczenie danych bez określenia sposobu – jeżeli osoba, której dane dotyczą wyśle je e-mailem, to robi to na własną odpowiedzialność (my o to nie prosiliśmy).



KORZYSTANIE ZE SŁUŻBOWEGO KOMPUTERA

- ☐ Nigdy nie należy otwierać załączników, ani klikać na linki w poczcie e-mail od nieznanych nadawców lub w wiadomościach, których się nie spodziewamy.
- ☐ Obowiązkiem pracownika jest korzystanie ze służbowego komputera oraz oprogramowania wyłącznie w celach wykonywania obowiązków pracowniczych.
- ☐ Nie wolno podłączać do portów USB lub wkładać do napędów DVD nośników zewnętrznych prywatnych lub pochodzących z nieznanego źródła.
- ☐ Podczas użytkowania komputera zabrania się wchodzenia na strony internetowe, które mogą stwarzać zagrożenie dla systemu informatycznego i bezpieczeństwa danych. **Nie surfuj po internetowych stronach o niewłaściwej treści, nie ściągaaj stamtąd żadnych plików.**
- ☐ Monitor komputera należy usytuować w taki sposób, aby osoby nieupoważnione wchodzące do pomieszczenia nie miały wglądu do danych na nim wyświetlanych.



Dziękuję za uwagę

Robert Wakoń

tel. +48 609 181 180

e-mail: r.wakon@rProtection.com.pl