RODO
słowniczek pojęć oraz podstawowe informacje

1. **Akty prawne regulujące prawo o ochronie danych osobowych:**
   a) **Rozporządzenie o ochronie danych osobowych lub 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) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.).

      Link do tekstu RODO - Baza Aktów Prawnych Unii Europejskiej:
      http://data.europa.eu/eli/reg/2016/679/oj

   b) Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. poz. 1000).
      Link do tekstu ustawy – Dziennik Ustaw:
      http://www.dziennikustaw.gov.pl/du/2018/1000/1

2. Kodeks branżowy dla podmiotów wykonujących działalność leczniczą – (PROJEKT)
   podstawa prawna: art. 40 RODO
   link do projektu z dnia 25 maja 2018 r. ze strony www.rodowzdrowiu.pl:

   http://www.rodowzdrowiu.pl/wp-content/uploads/2018/05/2018-05-25-RODO-DZP-kodeks-zmiany.docx

   http://www.rodowzdrowiu.pl/wp-content/uploads/2018/05/ROZDZIA%C5%81-5-RODO-wersja-V.docx

3. **Dane osobowe** - informacje, które pozwalają bezpośrednio lub pośrednio zidentyfikować osobę, np.:
   1. imię/nazwisko/adres
   2. imię/nazwisko/numer telefonu
   3. dane z bazy CEIDG
   4. e-maile (jan.nowak@energa.pl)
   5. monitoring, zapisy rozmów
   6. PESEL
   7. dane o lokalizacji
   8. adres IP, MAC

4. **Dane dotyczące zdrowia** - dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej - w tym o korzystaniu z usług opieki zdrowotnej - ujawniające informacje o stanie jej zdrowia.

5. **Dane wrażliwe** (szczególna kategoria danych):
    1. Dane dotyczące zdrowia fizycznego i psychicznego (dane medyczne, stopień niepełnosprawności, dyslekcja ucznia)
    2. Dane genetyczne (DNA, RNA, próbki biologiczne)
    3. Dane biometryczne (wizerunek lub dane daktyloskopijne)
    4. Wyroki skazujące i naruszenia prawa,
    5. Przynależność związkowa, polityczna, religijna, rasowa.

6. **Administrator** - organ, jednostka organizacyjna, podmiot lub osoba, decydująca o celach i środkach przetwarzania danych osobowych (firma, organizacja).

7. **Inspektor Ochrony Danych (IOD)** – koordynator wszelkich spraw związanych z danymi osobowymi w podmiocie. Nadzoruje, czy Administrator, wszyscy pracownicy i współpracownicy chronią dane w należyty sposób.

8. **Administrator Systemu Informatycznego** (ASI) – informatyk lub firma informatyczna odpowiedzialni za prawidłowe działanie i bezpieczeństwo infrastruktury IT.

9. **Formy występowania danych osobowych**:
    a) forma papierowa: akta osobowe, segregatory, archiwa, umowy z klientami, umowy-zlecenia, faktury,
    b) forma elektroniczna: programy kadrowo-płacowe, bazy klientów, dane na serwerze i na dyskach komputerów, pliki na pendrive,
    c) forma głosowa: centrala telefoniczna,
    d) forma wizyjna: monitoring wizyjny.

10. **Przetwarzanie danych** – operacje na danych osobowych, np.
    a) Wgląd
    b) Wprowadzanie
    c) Modyfikacja
    d) Usuwanie, niszczenie, anonimizacja
    e) Przetwarzanie na serwerze i w biurze
    f) Archiwizacja, kopie bezpieczeństwa.
    g) Udostępnianie, powierzanie, przesyłanie.

11. **Zbiór danych** - uporządkowany zestaw danych dostępnych według określonych kryteriów.
    Przykład: Zbiór pacjentów

12. **Przykładowa klauzula informacyjna dla pacjentów:**
    „Zgodnie z art. 13 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016) informuję, iż:
    1) administratorem Pani/Pana danych osobowych jest …. (*Nazwa i adres Administratora)*

2) kontakt z Inspektorem Ochrony Danych - iod@.....*(wskazanie adresu inspektora)*
3) Pani/Pana dane osobowe przetwarzane będą w celu świadczenia usług medycznych - na podstawie Art. 6 ust. 1 lit. c ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. oraz na podstawie Art. 9 ust.1 lit. h ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r
4) odbiorcami Pani/Pana danych osobowych będą wyłącznie podmioty uprawnione do uzyskania danych osobowych na podstawie przepisów prawa (NFZ) oraz laboratoria analityczne,
5) Pani/Pana dane osobowe przechowywane będą przez okres 20 lat/30 lat *(zgodnie z art. 29 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzecznik Praw Pacjenta (t.j. Dz. U. z 2017 r. poz. 1318 z późn. zm.).*
6) posiada Pani/Pan prawo do żądania od administratora dostępu do danych osobowych, ich sprostowania lub ograniczenia przetwarzania
7) ma Pani/Pan prawo wniesienia skargi do organu nadzorczego
8) podanie danych osobowych jest obligatoryjne na mocy przepisu prawa"

Sposób wprowadzenia klauzuli: Projekt kodeksu branżowego zaleca spełnienie obowiązku informacyjnego wobec pacjentów w przypadku zbierania danych osobowych bezpośrednio od nich (art. 13 RODO) w dwóch formach jednocześnie – np. w postaci wywieszki na tablicy ogłoszeń w przestrzeniach ogólnodostępnych oraz umieszczenie klauzul na stronach internetowych placówki (*Rozdział 5.3.2. projektu Kodeksu branżowego).*

13. **Naruszenie ochrony danych osobowych -** naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utraty, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych:
    a) pożar, zalanie,
    b) utrata danych (awarie, brak prądu, wirusy),
    c) świadome skasowanie danych ,
    d) włamanie lub kradzież danych,
    e) sprzedaż danych,
    f) przypadkowe usunięcie,
    g) przekazanie danych osobie nieupoważnionej
    h) zagubienie dokumentacji, laptopa, pendrive
    i) przypadkowa modyfikacja danych,
    j) upublicznienie danych w internecie
    k) nieuprawniony dostęp do danych osobowych

    Przykłady:
    - wysłanie danych do niewłaściwej osoby (np. poprzez niewłaściwie zaadresowanie poczty elektronicznej,
    - utrata nośników danych (telefon, laptop, USB, teczki zawierające dane w wersji papierowej)
    - nieuprawnione udostępnienie danych (np. elektronicznie – przekazywanie danych przez zdalny dostęp np. VPN, często przydzielane bezterminowo - ale też np. telefonicznie (rozmówca podaje się za pracownika policji czy urzędu, próbując wyciągnąć informacje);

- nieodpowiednie usuwanie danych (np. administrator postanawia pozbyć się starych komputerów; przed sprzedażą usuwa jedynie pliki na pulpicie i opróżnia kosz ze starych plików; nie usuwa jednak danych z dysku komputera).

14. Zgłoszenie naruszeń - w ciągu 72 godzin

IOD będzie miał obowiązek zgłaszania wszelkich naruszeń bezpieczeństwa danych osobowych w czasie do 72 godzin od naruszenia, bezpośrednio do właściwego organu nadzoru. Oznacza to, że każde naruszenie należy zgłosić bezpośrednio do organu nadzorczego w nieprzekraczalnym czasie 72 godzin i to niezależnie od powiadomienia przełożonych.
W niektórych przypadkach należy również poinformować o takim incydencie konkretne osoby, których dane „wyciekły".

Wzór powiadomienia o naruszeniu – zgłoszenie do organu przygotowane w ramach projektu kodeksu branżowego:

„Nazwa administratora danych (Administrator):
Dane kontaktowe inspektora ds. ochrony danych: [imię, nazwisko, dane kontaktowe, adres e-mail, numer telefonu]
Data i godzina powiadomienia:

ZGŁOSZENIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH
Działając na podstawie art. 33 ust. 1 RODO, Administrator niniejszym zgłasza przypadek naruszenia ochrony danych osobowych.

(a) Charakter naruszenia:
Data i godzina stwierdzenia naruszenia
Opis charakteru naruszenia
Kategoria osób, których dane zostały naruszone
Przybliżona liczba osób, których dane zostały naruszone
Kategorie wpisów danych osobowych, których dotyczy naruszenie
Przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie

Możliwe konsekwencje naruszenia ochrony danych osobowych
Środki zastosowane przez Administratora w celu zaradzenia naruszeniu ochrony danych osobowych
(należy wskazać również czy poinformowano osoby, których dane dotyczą)

Środki proponowane przez Administratora w celu zminimalizowania ew. negatywnych skutków naruszenia

Zgłoszenie zawiera opis stanu faktycznego na dzień jego sporządzenia i w razie pojawienia się nowych okoliczności w sprawie, mających istotny wpływ na opisany powyżej charakter naruszenia, zgłoszenie może zostać zaktualizowane.
Jednocześnie, z uwagi na upływ 72 h od stwierdzenia naruszenia, Administrator wyjaśnia, iż przyczyną opóźnienia przekazania niniejszego zgłoszenia jest […]."

Link do formularza zgłoszenia naruszenia ze strony Urzędu Ochrony Danych Osobowych https://uodo.gov.pl/data/filemanager_pl/770.docx

15. **Bezpośrednia odpowiedzialność przetwarzającego dane -**za naruszenie przepisów o ochronie danych osobowych odpowiadać będzie administrator (szef firmy, jednostki, szkoły, urzędu). Odpowiedzialność jest bezpośrednia i powołanie inspektora ochrony danych osobowych, czy wynajęcie firmy zewnętrznej w tym obszarze, nie zwalnia z tej odpowiedzialności.

16. **Siedem zasad RODO:**

1. Zasada zgodności z prawem, przejrzystości i rzetelności. (art. 5 ust. 1 pkt a) RODO):

Dane osobowe muszą być:
przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość").
Zbieranie danych osobowych musi mieć określoną podstawę prawną (zgoda osoby, przepis prawa).
Prawidłowa realizacja obowiązków informacyjnych jest warunkiem niezbędnym dla osiągnięcia zgodności z zasadą rzetelności i przejrzystości.

2. Zasada ograniczenia celu przetwarzania (art. 5 ust. 1 lit. b) RODO):

Dane osobowe muszą być:
zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami („ograniczenie celu");
Cel zbierania danych musi być czytelnie zakomunikowany osobie, której dane dotyczą jeszcze przed faktycznym zebraniem od niej danych osobowych.
Danych zebranych w określonym celu nie można przetwarzać w innym bez zgody osoby.

3. Zasada minimalizacji danych (art. 5 ust. 1 lit. c) RODO):
art. 5 ust. 1 lit. c

Dane osobowe muszą być: (…)
adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych");
Zakres przetwarzanych danych powinien być taki jaki jest niezbędny do osiągnięcia określonego celu przetwarzania danych.
Każdy podmiot przetwarzający dane musi dokonać selekcji danych i wybrać tylko taką ich ilość oraz rodzaj jakie są dla niego niezbędne.

4. **Zasada prawidłowości danych (art. 5 ust. 1 lit. d) RODO):**

Dane osobowe muszą być: (…)
prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość");

Przestrzeganie zasady prawidłowości danych sprowadza się do tego, aby stworzone zostały odpowiednie rozwiązania techniczne oraz organizacyjne umożliwiające korygowanie nieprawidłowych lub nieaktualnych danych**.**

5. **Zasada ograniczenia przechowywania danych (art. 5 ust. 1 lit. e) RODO):**

Dane osobowe muszą być:
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; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania");
Realizacja tej zasady jest możliwa poprzez wdrożenie odpowiednich procedur wyznaczających terminy przechowania danych lub procedur określających terminy okresowych przeglądów danych.

6. **Zasada integralności i poufności (art. 5 ust. 1 lit. f) RODO):**

Dane osobowe muszą być:
przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").
Realizacja zasady integralności i poufności danych polega na wdrożeniu odpowiednich środków technicznych i organizacyjnych, które zapewnią bezpieczeństwo danych. „Odpowiednie środki" będą zawsze pojęciem niedookreślonym. Najprawdopodobniej zostaną w pewnym zakresie doprecyzowane w drodze dobrych praktyk, które ma wydać regulator – Prezes Urzędu Ochrony Danych Osobowych

7. **Zasada rozliczalności (art. 5 ust. 2 RODO):**

Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie („rozliczalność").

Administrator będzie więc musiał wykazać, że określone decyzje odnoszące się do procesów przetwarzania danych osobowych zostały przeanalizowane z punktu widzenia zgodności z ogólnymi zasadami przetwarzania danych, a przede wszystkim, że są z nimi zgodne.

17. Dane kontaktowe Urzędu Ochrony Danych Osobowych: https://uodo.gov.pl/

ul. Stawki 2
00-193 Warszawa
tel. 22 531 03 00
fax. 22 531 03 01
https://www.uodo.gov.pl/pl/p/kontakt