

**ALP****American
Heart of Poland**

Gruppo San Donato



OCHRONA DANYCH OSOBOWYCH - W PIGUŁCE

PRZEPISY

- 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 – rozpoczęcie stosowania od 25 maja 2018 r.
- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych
- Ustawa o prawach pacjenta i Rzeczniku Praw Pacjenta

WEWNĘTRZNE PROCEDURY - min.:

- Podręcznik Bezpieczeństwa
- Polityka Bezpieczeństwa Danych Osobowych
- Zarządzanie incydentami bezpieczeństwa informacji

DEFINICJE:

DANE OSOBOWE – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, zidentyfikowanej pośrednio lub bezpośrednio 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.

- **Dane osobowe zwykłe** – np.: imię, nazwisko, adres zamieszkania, telefon, PESEL, email, adres IP komputera, dane o lokalizacji GPS, nr rejestracyjny samochodu, nr księgi głównej w medycznym systemie informatycznym.
- **Szczególna kategoria danych (dane „wrażliwe”)** – dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne, dane dotyczące zdrowia, seksualności lub orientacji seksualnej osoby.
- **Dane dotyczące wyroków skazujących i naruszeń prawa.**

PRZETWARZANIE DANYCH OSOBOWYCH - zautomatyzowane lub niezautomatyzowane operacje na danych osobowych lub zestawach danych osobowych takie jak:

- zbieranie, utrwalanie, organizowanie, porządkowanie, adoptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, rozpowszechnianie lub innego rodzaju udostępnienie, ujawnianie poprzez przesyłanie (mail, kurier), dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

ADMINISTRATOR DANYCH OSOBOWYCH - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. W naszym przypadku: AMERICAN HEART OF POLAND S.A.

INSPEKTOR OCHRONY DANYCH - osoba wyznaczona przez administratora bądź podmiot przetwarzający. Inspektor ochrony danych bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego.

Kontakt z IOD: rodo@ahop.pl



ZAPEWNIENIE BEZPIECZEŃSTWA

Zapewnienie bezpieczeństwa fizycznego:

- ochrona pomieszczeń,
- monitoring,
- kontrola dostępu,
- pomieszczenia zamykane na klucz,
- szafy i biurka zamykane na klucz.

Zapewnienie bezpieczeństwa organizacyjnego:

- zabezpieczenie kluczy,
- polityka czystego biurka (w zasięgu ręki i wzroku),
- drukarki i ksera zabezpieczone przed dostępem osób postronnych,
- niszczenie dokumentów w niszczarkach,
- sprząatanie w obecności pracowników,
- zabezpieczenie dokumentów i nośników **przy wynoszeniu** poza teren miejsca pracy.

Zapewnienie bezpieczeństwa informatycznego:

- logowanie **zawsze** na swój login i hasło,
- indywidualna **odpowiedzialność** za wszystkie działania wykonane z wykorzystaniem osobistego loginu i hasła,
- **blokowanie komputera**,
- stosowanie **wygaszacza** ekranu z hasłem po czasowym odejściu od stanowiska pracy, ochrona przed osobami postronnymi,
- po zakończeniu pracy **wylogować się i wyłączyć** komputer,
- w razie awarii komputera powiadomić IT,
- **nie otwierać** podejrzanych załączników otrzymanych emailem,
- hasłować pliki zawierające **dane osobowe** (hasła wysłać inną formą komunikacji – telefon, SMS),
- wysyłając maile pamiętać o opcjach: do wiadomości (**DW**) oraz do ukrytej wiadomości (**UDW**) – w przypadku zbiorczych maili wysyłanych na prywatne skrzynki mailowe,
- polityka czystego ekranu,
- **nie wolno instalować** ani nie używać żadnych programów na komputerach firmowych bez uzyskania zgody IT,
- **nie należy wyłączać** programu antywirusowego.

POLITYKA HASEŁ

- hasła nie mogą być zapisywane na kartkach, naklejane na komputer, trzymane pod klawiaturą lub w szufladzie,
- **zakaz** udostępniania swojego hasła, a w przypadku ujawnienia hasła - natychmiastowa zmiana,
- hasła powinny składać się z co najmniej **12 znaków**,
- **duże litery + małe litery + cyfry/znaki specjalne**,
- hasła muszą być **zmieniane cyklicznie**.



ZAGROŻENIA ZWIĄZANE Z BEZPIECZEŃSTWEM DANYCH

- nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł itd.),
- niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
- nieodpowiednie zabezpieczenie sprzętu IT czy oprogramowania przed wyciekiem lub utratą danych osobowych.

INCYDENTY ZWIĄZANE Z BEZPIECZEŃSTWEM DANYCH to pojedyncze zdarzenie lub seria niepożądanych albo niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.

Zasadnicze grupy incydentów w ochronie danych osobowych:

- umyślne incydenty (np. kradzież danych i sprzętu, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie danych, włamanie do systemu informatycznego lub pomieszczeń),
- zdarzenia losowe wewnętrzne (np. awaria komputera/serwera/dysku twardego/oprogramowania, pomyłki informatyków, utrata danych),
- zdarzenia losowe zewnętrzne (np. pożar, zalanie wodą, utrata zasilania, utrata łączności).

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH

Wszystkie osoby mające dostęp do danych osobowych mogą je przetwarzać działając z upoważnienia administratora danych lub podmiotu przetwarzającego – wyłącznie na polecenie administratora.

OBOWIĄZKI PRACOWNICZE

Konieczność stosowania się do zasad bezpieczeństwa przyjętych w organizacji. W razie wystąpienia incydentów związanych z ochroną danych osobowych, pracownik powinien je zidentyfikować i zgłosić swojemu przełożonemu lub Inspektorowi Ochrony Danych.

KARY

DLA ADMINISTRATORA DANYCH

- **Odpowiedzialność finansowa:** Zależnie od okoliczności, za naruszenie przepisów ochrony danych osobowych może zostać nałożona kara pieniężna w wysokości do 20 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

- **Odpowiedzialność karna:** Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch, w przypadku szczególnych kategorii danych do lat trzech.

DLA PRACOWNIKA

(może, ale nie musi być zastosowana – decyzja należy do Administratora danych)

- **Odpowiedzialność porządkowa:** Nawet jeśli pracodawca nie został ukarany za naruszenie ochrony danych osobowych spowodowanych przez pracownika, to i tak pracownik może zostać ukarany karą porządkową upomnienia lub nagany za naruszenie porządku pracy. Kara ulega zatarciu (usunięciu z akt osobowych pracownika) po roku nienaganej pracy.
- **Zwolnienie dyscyplinarne:** W skrajnych przypadkach, jeżeli uchybienie pracownika będzie nosiło znamiona ciężkiego naruszenia podstawowych obowiązków pracowniczych, pracodawca może rozwiązać z pracownikiem umowę o pracę bez wypowiedzenia.
- **Odpowiedzialność materialna:** Jeżeli przez naruszenie (zaniechanie pracownika) doszło do wyrządzenia szkody pracodawcy (pracodawca został obciążony karą pieniężną przez Prezesa UODO lub musiał zapłacić odszkodowanie podmiotowi danych), wówczas w trybie roszczenia regresowego pracodawca może zażądać odszkodowania od pracownika. W przypadku wyrządzenia szkody z winy nieumyślnej odszkodowanie nie może przekraczać równowartości 3-miesięcznego wynagrodzenia pracownika. Limit nie dotyczy naruszeń umyślnych. Pracodawca może dochodzić odszkodowania na drodze sądowej.

