Lotnicze Pogotowie Ratunkowe

PODSTAWOWE ZASADY OCHRONY DANYCH OSOBOWYCH

Ogólne Rozporządzenie o ochronie danych osobowych (RODO)

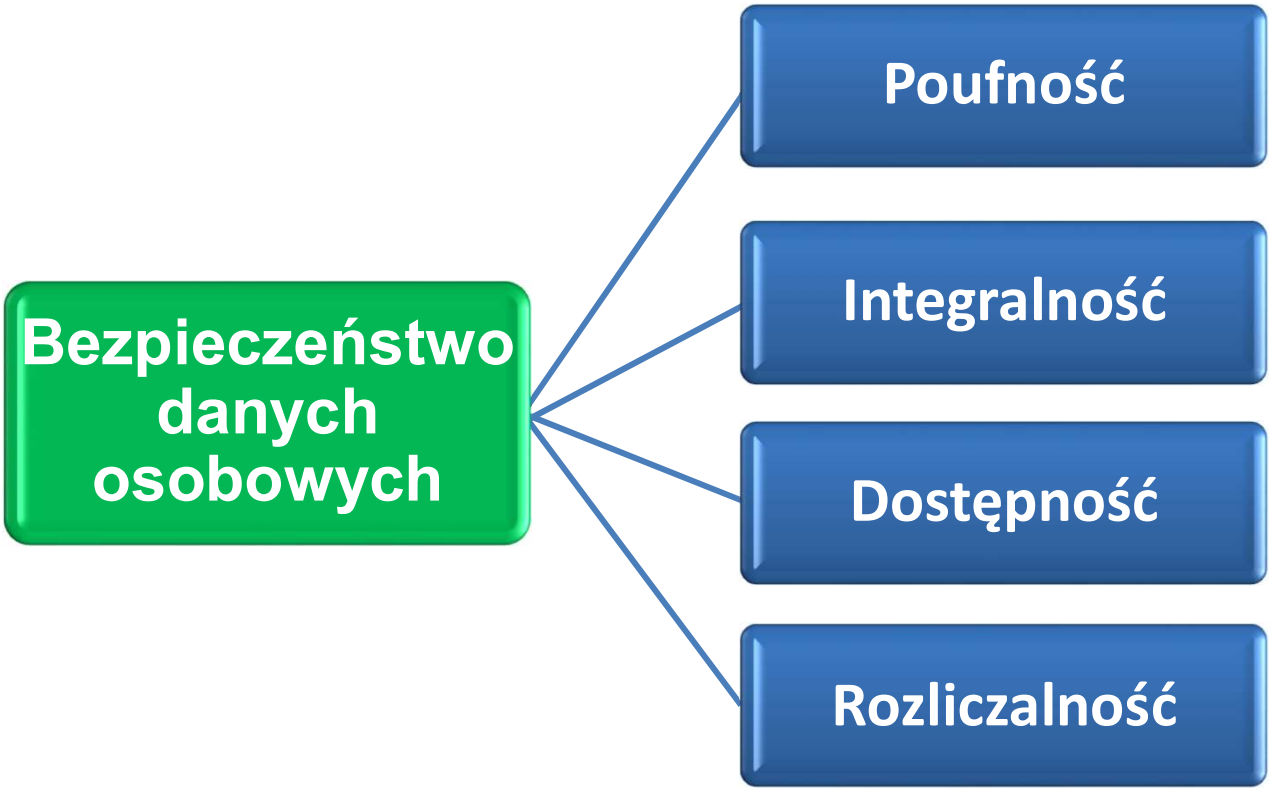
Od kiedy jest stosowane?

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

RODO, GDPR, ogólne rozporządzenie o ochronie danych

Rozporządzenie stosuje się od dnia 25 maja 2018 r.

Podstawowe pojęcia



Podstawowe zasady dotyczące przetwarzania danych

Dane należy przetwarzać zgodnie z następującymi zasadami:

1. Zgodność z prawem, rzetelność i przejrzystość.
2. Ograniczenie celu.
3. Minimalizację danych.
4. Prawidłowość.
5. Ograniczenie przechowywania.
6. Integralność i poufność.

Podstawowe Definicje

Dane osobowe

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:

1. imię i nazwisko,
2. numer identyfikacyjny,
3. dane o lokalizacji,
4. identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

PRZYKŁAD – imię i nazwisko, nr PESEL, nr telefonu, adres e-mail, jeżeli jesteśmy w stanie przyporządkować te dane do konkretnej osoby.

Podstawowe Definicje

Dane szczególnych kategorii

Dane szczególnych kategorii - Szczególne kategorie danych (dane wrażliwe) - dane osobowe ujawniające:

1. pochodzenie rasowe lub etniczne;
2. poglądy polityczne;
3. przekonania religijne lub światopoglądowe;
4. przynależność do związków zawodowych;
5. przetwarzanie danych genetycznych i danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby;

Tzw. dane „karne”, czyli dane dotyczące wyroków skazujących.
PRZYKŁAD informacje o stanie zdrowia.

UWAGA! Powyższe przykłady stanowią katalog zamknięty.

Podstawowe Definicje

Przetwarzanie 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;

PRZYKŁAD – zapisywanie danych na kartce papieru, zapisywanie dokumentów w systemie, archiwizowanie dokumentacji, kopiowanie i kserowanie dokumentacji, etc.

Podstawowe Definicje

Administrator

Administrator – Osoba fizyczna lub prawna, organ publiczny, jednostka organizacyjna lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele przetwarzania danych osobowych.

Administratorem zawsze jest organizacja, a nie osoba nią zarządzająca (np. dyrektor, członek zarządu).

Podmiot przetwarzający

Oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora.

Podmiot przetwarzający samodzielnie nie ustala celów przetwarzania danych osobowych.

Artykuł 28 RODO

- obowiązek zawarcia umowy powierzenia przetwarzania z
- podmiotem przetwarzającym;
- umowa określa m.in. zakres powierzonych do przetwarzania danych, cele przetwarzania, rodzaj i kategorie danych, możliwość przeprowadzenia kontroli, pomoc w realizacji praw, obowiązek zgłaszania naruszeń, obowiązek odpowiedniego zabezpieczenia danych;

Powierzenie danych osobowych

Zatem w myśl przepisów RODO, konieczność zawarcia umowy powierzenia przetwarzania danych osobowych istnieje wówczas, gdy administrator zleca wykonywanie swoich zadań innemu podmiotowi (podmiotowi przetwarzającemu).

Z jakimi podmiotami najczęściej zawieramy umowę powierzenia?

Hostingodawcy

Serwisanci np. Sprzętu it, sprzętu diagnostycznego;

Usługodawcy np. Księgowi

Podmioty zajmujące się archiwizacją i brakowaniem dokumentacji;

Umowy zawierane z podmiotami na świadczenie różnych usług powinny być konsultowane z IOD w zakresie konieczności podpisania umowy powierzenia danych osobowych.

UMOWY POWIERZENIA DANYCH POWINNY BYĆ PRZEKAZYWANE DO IOD W CELU UJĘCIA W REJESTRZE UMÓW POWIERZENIA .

Prawa przysługujące osobom, których dane są przetwarzane.

1. Prawo do bycia poinformowanym.
2. Prawo dostępu do danych.
3. Prawo do sprostowania/uzupełnienia danych.
4. Prawo do usunięcia danych (prawo do bycia zapomnianym).
5. Prawo do ograniczenia przetwarzania danych.
6. Prawo do przenoszenia danych.
7. Prawo do sprzeciwu wobec przetwarzania danych.
8. Prawo do niepodlegania decyzji opartej wyłącznie na zautomatyzowanym przetwarzaniu.

Realizacja praw

- **Weryfikujemy** tożsamość Wnioskodawcy;
- Ustalamy, czy Wnioskodawcy przysługuje wskazane prawo;
- **Termin w którym realizujemy wniosek wynosi miesiąc**, w szczególnie skomplikowanych sprawach 3 miesiące, ale musimy poinformować o tym Wnioskodawcę;
- W przypadku wpływu wniosku informujemy o tym niezwłocznie IOD;

Ochrona dokumentów

- Dokumenty powinny być przechowywane w pomieszczeniach i sprzętach gwarantujących bezpieczeństwo i zapewniających kontrolę dostępu (np. zamykane w szafach, przechowywane w teczkach, posegregowane w sposób ułatwiający ich odnalezienie, dokumenty podlegające szczególnej ochronie powinny być przechowywane w miejscach, do których dostęp mają jedynie osoby upoważnione do ich przetwarzania).
- Dokumenty przesyłane w postaci elektronicznej muszą być szyfrowane w sposób uzgodniony z adresatem, gwarantujący ich poufność.

Ochrona dokumentów

Dane osobowe mogą być przetwarzane wyłącznie w obszarach przetwarzania danych osobowych, na które składają się **pomieszczenia biurowe** oraz **części pomieszczeń, gdzie LPR prowadzi działalność**. Do takich pomieszczeń, zalicza się w szczególności:

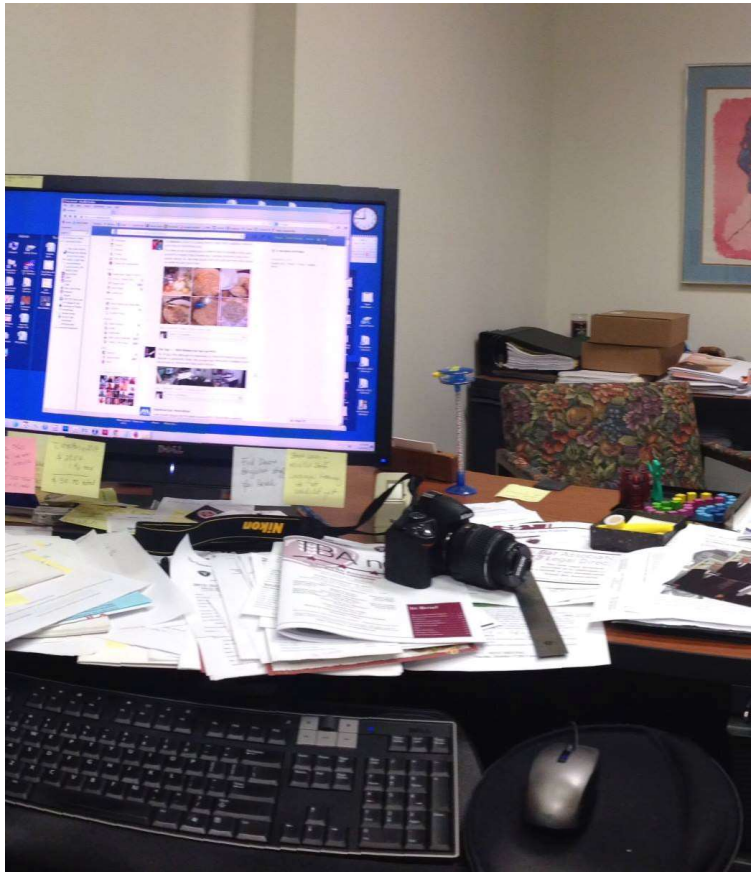
- pomieszczenia biurowe, w których zlokalizowane są stacje robocze lub serwery służące do przetwarzania danych osobowych;
- pomieszczenia, w których przechowuje się dokumenty źródłowe oraz wydruki z systemu informatycznego zawierające dane osobowe;
- pomieszczenia, w których przechowywane są sprawne i uszkodzone urządzenia, elektroniczne nośniki informacji oraz kopie zapasowe zawierające dane osobowe.

Ochrona dokumentów

Pomieszczenia, w których są przetwarzane dane osobowe powinny być na czas nieobecności pracowników upoważnionych do przetwarzania tych danych osobowych zamykane na klucz w sposób uniemożliwiający dostęp osobom nieupoważnionym.

Zaleca się, aby przed wyjściem uprzątnąć również dokumentację znajdującą się na biurkach oraz zamknąć ją w szufladach/szafach.

Ochrona dokumentów



UWAGA!!

- Nie należy pozostawiać dokumentacji na biurkach oraz w miejscach ogólnodostępnych. Przed opuszczeniem stanowiska należy schować dokumenty np. do szuflady.

- Należy również pamiętać o zachowaniu porządku na pulpicie systemu, nie przechowując na nim ważnej dokumentacji. Zaleca się, aby taka dokumentacja znajdowała się „głębiej” w folderach.

- Dokumentacji nie należy wynosić poza obszar LPR bez zgody Administratora.

Ochrona dokumentów

Dokumenty, które straciły ważność lub przydatność należy niszczyć przy użyciu niszczarki.

UWAGA!!!
Nie należy dokumentów zgniatać lub rozdzierać ręcznie i wyrzucać do kosza, ponieważ nadal istnieje możliwość odtworzenia takich dokumentów przez osoby nieuprawnione.

Bezpieczeństwo poczty e-mail

- Należy zawsze pilnować poufności hasła do swojego konta na poczcie e-mail.
- Za każdym razem należy weryfikować adres e-mail odbiorcy oraz treść przesyłanego maila wraz z załącznikami.
- Pamiętaj, aby szczególnie ważne informacje, przesyłane drogą mailową były szyfrowane, a hasło zostało przesłane odrębnym kanałem komunikacji.

Bezpieczeństwo poczty e-mail

- Nie należy otwierać wiadomości od podejrzanych nadawców.
- Nie pobieraj i nie otwieraj podejrzanych załączników.
- Należy zachować szczególną ostrożność w przypadku podejrzanie wyglądającej treści maila (np. mail, z którego wynika, że właśnie coś wygrałeś i aby sfinalizować transakcję, potrzebne są Twoje dane).
- W takim przypadku szczególną uwagę należy zwrócić na rozszerzenie załącznika, gdyż może to być zarówno plik .exe , jak i .html, .bat, .pak, .jar lub posiadać inne, nietypowe rozszerzenia.

Ochrona stanowiska komputerowego

- Należy pamiętać o cyklicznej zmianie hasła do systemu.
- Zabrania się instalowania na sprzęcie komputerowym jakiegokolwiek oprogramowania bez wiedzy i zezwolenia Przełożonego
- Opuszczając stanowisko należy za każdym razem blokować dostęp do systemu (skrót Win. + L).
- Jeżeli użytkownik korzysta z laptopa, należy wylogować się z systemu lub zamknąć system, następnie zamknąć laptopa i schować w miejscu, w którym sprzęt będzie bezpieczny (np. z dala od promieni słonecznych, kaloryfera, miejsc grożących zalaniem itp.

Ochrona stanowiska komputerowego

- Nie należy stosować hasła, które łatwo powiązać z Użytkownikiem (np. imię i nazwisko, imię psa, ulubiony zespół muzyczny itp.).
- Należy unikać zapisywania swojego hasła na karteczkach lub w notatniku.
- Utworzone przez użytkownika hasło musi:
  - ✓ Składać się min. z 9 znaków;
  - ✓ Posiadać małe i duże litery;
  - ✓ Posiadać cyfry;
  - ✓ Posiadać znak specjalny;
  - ✓ Być unikalne i niepowtarzalne.

Ochrona stanowiska komputerowego

- Należy regularnie upewniać się, iż system posiada aktywną ochronę sieciową (np. w postaci antywirusa).
- Należy pamiętać o regularnych aktualizacjach systemu oraz oprogramowania, pozwoli to uchronić się przed aktualnymi zagrożeniami.

Domyślna ochrona danych

Osoby upoważnione do przetwarzania danych osobowych są zobowiązane do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których uzyskały dostęp w trakcie zatrudnienia, również po ustaniu zatrudnienia.

Drukowanie dokumentacji

- ZAWSZE należy odbierać swoje wydruki z drukarki. Jeśli są nieprawidłowe lub niezdatne należy zniszczyć je za pomocą niszczarki,
- Należy pamiętać, aby nie zostawiać dokumentów na szybie skanera,
- Nie należy używać prywatnych nośników.
- Nie należy zostawiać dokumentacji bez nadzoru w miejscach ogólnodostępnych.

Zdarzenia/ incydenty

incydent

- Przez incydent rozumiane jest zdarzenie, które może mieć negatywny wpływ na działanie Organizacji

Każdy Pracownik oraz współpracownik LPR ma obowiązek niezwłocznego zgłoszenia podejrzenia wystąpienia lub stwierdzenia wystąpienia zdarzenia/ incydentu, złożenie notatki w zakresie zgłaszanego incydentu nie powinno nastąpić później niż 24 godziny od chwili stwierdzenia wystąpienia lub podejrzenia wystąpienia incydentu.

Zgłaszanie zdarzeń/ incydentów

Wszystkie zdarzenia/incydenty związane z bezpieczeństwem zgłaszamy niezwłocznie do IOD:

- Pocztą elektroniczną – na adres: **iod@lpr.com.pl**
- Telefonicznie – pod numerem: **785 390 188**
- Osobiście – w siedzibie **LPR**,

Zdarzenia/incydenty związane z bezpieczeństwem fizycznym

- Zgubienie kluczy lub kart dostępowych do pomieszczeń;
- Zgubienie/ kradzież dokumentów należących do LPR;
- Zniszczenie dokumentów należących do LPR;
- Pozostawienie otwartego pokoju/ okien w pokoju po zakończeniu pracy;
- Wejście do pomieszczeń z pominięciem kontroli dostępu;
- Identyfikacja na terenie LPR osoby nieuprawnionej do przebywania w danej lokalizacji, poruszającej się w sposób swobodny;
- Zgubienie/ kradzież/ zniszczenie nośnika.

Zdarzenia/incydenty związane z bezpieczeństwem informatycznym:

- Zidentyfikowanie złośliwego oprogramowania na stacji roboczej użytkownika;
- Zidentyfikowanie ataku hakerskiego;
- Niestabilna praca zasobów teleinformatycznych;
- Zbyt duże obciążenie procesora stacji roboczej lub innego urządzenia elektronicznego;
- Usunięcie danych;
- Brak aktualnych kopii bezpieczeństwa;
- Zidentyfikowanie prób omijania zabezpieczeń systemów informatycznych;
- Identyfikacja nieznanych nośników wpiętych do urządzeń np. do drukarek, laptopów.

Inne zdarzenia/incydenty:

- Pozostawienie nośników bez nadzoru;
- Kradzież służbowego telefonu;
- Przypadkowe ujawnienie loginu i hasła do systemów informatycznych;
- Przesłanie wiadomości e-mail do niewłaściwego adresata;
- Ujawnienie informacji poufnych osobom nieuprawnionym do uzyskania dostępu do w/w informacji;
- Skopiowanie danych przez osobę do tego nieuprawnioną.

Odpowiedzialność pracowników LPR za niewłaściwe zabezpieczenie danych

Odpowiedzialność dyscyplinarna

Przetwarzanie danych osobowych z naruszeniem upoważnienia do przetwarzania danych udzielonego przez pracodawcę może stanowić uzasadnioną przyczynę rozwiązania umowy o pracę (wyrok Sądu Najwyższego z 4 kwietnia 2017 r., II PK 37/16).

Odpowiedzialność cywilna

Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny

- Art. 448. **W razie naruszenia dobra osobistego sąd może przyznać temu, czyje dobro osobiste zostało naruszone, odpowiednią sumę tytułem zadośćuczynienia pieniężnego za doznaną krzywdę lub na jego żądanie zasądzić odpowiednią sumę pieniężną na wskazany przez niego cel społeczny, niezależnie od innych środków potrzebnych do usunięcia skutków naruszenia. Przepis art. 445 § 3 stosuje się.**
- Przez krzywdę rozumie się ból, cierpienie psychiczne, moralne.

Odpowiedzialność – ustawa o ochronie danych osobowych

- Art. 107. 1. **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.**
- 2. Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych genetycznych, danych biometrycznych przetwarzanych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, seksualności lub orientacji seksualnej, podlega grzywnie, **karze ograniczenia wolności albo pozbawienia wolności do lat trzech.**
- Art. 108. Kto udaremnia lub utrudnia kontrolującemu prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych, **podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.**

Dziękujemy za uwagę