Informacje z zakresu ochrony danych osobowych, w tym z zakresu przepisów RODO

Podstawa prawna

1. 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)
2. Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta
3. Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia
4. Regulacje wewnętrzne: Regulaminy, Procedury, Instrukcje.

Podstawowe definicje związane z ochroną danych osobowych

RODO - oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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.Urz. UE L 119, s. 1).

Administrator - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych - Wojewódzkie Centrum Szpitalne Kotliny Jeleniogórskiej w Jeleniej Górze.

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.

Przetwarzanie - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką 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.

Dane wrażliwe - oznaczają dane o szczególnych kategoriach oraz dane karne.

Szczególne kategorie danych - oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej.

Dodatkowych informacji udziela IOD – Małgorzata Bielecka, wew. 7259, pok. 21a

Dane karne oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa.

Osoba - oznacza osobę fizyczną, której dane dotyczą.

Podmiot przetwarzający - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora; Podmiot przetwarzający jest odrębnym bytem prawnym. Może wykonywać operacje przetwarzania jedynie na udokumentowane polecenie Administratora. W obszarze ISO podmiot ten najczęściej nazywany jest – procesorem.

Odbiorca - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są uznawane za odbiorców.

Czynność przetwarzania - oznacza mniejszy lub większy (krótszy lub dłuższy) wycinek procesu „biznesowego”/ procesu przetwarzania danych realizowanego w konkretnym celu przetwarzania danych. Czynności przetwarzania danych składają się z operacji przetwarzania danych.

Profilowanie - oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

IOD lub Inspektor - oznacza Inspektora Ochrony Danych Osobowych

Zagrożenie – jest to potencjalna przyczyna niepożądanego incydentu, który może powodować szkody dla systemu lub organizacji. Incydenty powstają wskutek zagrożeń. Na zagrożenie i jego prawdopodobieństwo mają wpływ: okoliczności, stan prawny, stan faktyczny, działania, zaniechanie działań i wydarzenia zewnętrzne oraz wewnętrzne, które mogą ale nie muszą wywołać ryzyko wystąpienia incydentu.

Incydent bezpieczeństwa informacji - jest zdarzeniem, którego bezpośrednim lub pośrednim skutkiem jest lub może być naruszenie ochrony danych osobowych.

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;

Pseudonimizacja - oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

Zgoda - osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;

Dane dotyczące zdrowia - oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej - w tym o korzystaniu z usług opieki zdrowotnej - ujawniające informacje o stanie jej zdrowia; Zgodnie z Preambułą w motywie (35) - do danych osobowych dotyczących zdrowia należy zaliczyć wszystkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia osoby, której dane dotyczą. Do danych takich należą informacje o danej osobie fizycznej zbierane podczas jej rejestracji do usług opieki zdrowotnej lub podczas świadczenia jej usług opieki zdrowotnej, jak to określa dyrektywa Parlamentu Europejskiego i Rady 2011/24/UE; numer, symbol lub oznaczenie przypisane danej osobie fizycznej w celu jednoznacznego zidentyfikowania tej osoby fizycznej do celów zdrowotnych; informacje pochodzące z badań laboratoryjnych lub lekarskich części ciała lub płynów ustrojowych, w tym danych genetycznych i próbek biologicznych; oraz wszelkie informacje, na przykład o chorobie, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu klinicznym lub stanie fizjologicznym lub biomedycznym osoby, której dane dotyczą, niezależnie od ich źródła, którym może być na przykład lekarz lub inny pracownik służby zdrowia, szpital, urządzenie medyczne lub badanie diagnostyczne in vitro.

Prawa i obowiązków Administratora Danych Osobowych;

Administrator - Wojewódzkie Centrum Szpitalne Kotliny Jeleniogórskiej w Jeleniej Górze, oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.
1. Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
2. Administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, o których mowa w ust. 1.

Prawa i obowiązki Inspektora Ochrony Danych

1. Informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
2. Monitorowanie przestrzegania RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
3. Pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia.
4. Prowadzenie rejestru czynności lub rejestru kategorii czynności

Zasady udostępniania i powierzania danych osobowych

1. Dane osobowe udostępniane są upoważnionym osobom i uprawnionym instytucjom.
2. Powierzenie przetwarzania danych osobowych następuje w drodze umowy powierzenia.

Reguła czystego biurka

1. Dokumenty i wydruki trwale przechowuje się w archiwum lub w zabezpieczonych fizycznie pomieszczeniach, biurkach, szafach itp.
2. Osoby upoważnione zobowiązane są do zabezpieczenia dokumentów przed dostępem osób nieupoważnionych podczas swojej nieobecności w pomieszczeniach lub po zakończeniu pracy.
3. Wydruki nie mogą pozostawać na ksero, drukarkach, skanerach i kserokopiarkach bez nadzoru.
4. Osoby uprawnione są zobowiązane do niszczenia dokumentów i tymczasowych wydruków w niszczarkach niezwłocznie po ustaniu celu ich przetwarzania.
5. Nośniki informacji należy umieścić w szafach, szufladach i innych do tego przeznaczonych miejscach oraz upewnić się, że pokój jest zamknięty, gdy jesteśmy jedyną osobą opuszczającą pomieszczenie

Reguła czystego ekranu

1. Przed zalogowaniem się do systemu stacji roboczej należy upewnić się, że w pobliżu nie ma osób trzecich lub urządzeń nagrywających mogących zarejestrować hasła dostępowe do systemów, z których zamierzamy skorzystać. Jeśli występuje takie zagrożenie należy zastosować szczególne środki ostrożności uniemożliwiające zarejestrowanie wpisywanego hasła.;
2. Monitor należy usytuować w taki sposób, aby osoby nieupoważnione wchodzące do pomieszczenia nie miały wglądu do danych na nim wyświetlanych;
3. Używanych identyfikatorów i haseł nie należy udostępniać innym osobom, a w przypadku podejrzenia, że osoba postronna weszła w ich posiadanie, należy dokonać ich zmiany zgodnie z obowiązującymi procedurami;
4. Po zakończeniu pracy należy wylogować się ze wszystkich systemów, z których korzystaliśmy;
5. W przypadku opuszczania stanowiska pracy należy zastosować systemową blokadę komputera, laptopa lub innego elektronicznego nośnika informacji

Zasada tworzenia bezpiecznego hasła

1. Hasło dostępu do zbioru danych składa się co najmniej z 8 znaków (dużych i małych liter oraz z cyfr lub znaków specjalnych).
2. Zmiana hasła do systemu następuje nie rzadziej, niż co 30 dni oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione.
3. Zmianę hasła wymusza system lub użytkownik zobowiązany jest do manualnej zmiany hasła.

4. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.
5. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.
6. Zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom.

Praca w internecie

1. Użytkownicy mają prawo korzystać z Internetu w celu wykonywania obowiązków służbowych.
2. Przy korzystaniu z Internetu, użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i praw autorskich.
3. Użytkownicy nie mają prawa korzystać z Internetu dla celów prywatnych.
4. Użytkownicy nie mają prawa korzystać z Internetu w celu przeglądania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec obowiązujących zasad postępowania, a także grać w gry komputerowe w Internecie lub w systemie informatycznym Pracodawcy, ściągać z Internetu jakichkolwiek plików muzycznych lub wideo.

W zakresie dozwolonym przepisami prawa, Pracodawca zastrzega sobie prawo kontrolowania sposobu korzystania przez Użytkownika z Internetu pod kątem wyżej opisanych zasad. Ponadto, w uzasadnionym zakresie, Pracodawca zastrzega sobie prawo kontroli czasu spędzanego przez Użytkownika w Internecie. Pracodawca może również blokować dostęp do niektórych treści dostępnych przez Internet.

Zasady postępowania w sytuacji naruszenia ochrony danych osobowych

Użytkownik zobowiązany jest do powiadomienia bezpośredniego przełożonego, Inspektora Ochrony Danych w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych.

Typowe sytuacje, gdy użytkownik powinien powiadomić IOD:

1. ślady na drzwiach, oknach i szafach wskazują na próbę włamania;
2. dokumentacja jest niszczona bez użycia niszczarki;
3. fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie;
4. otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe;
5. ustawienie monitorów pozwala na wgląd osób postronnych na dane osobowe;
6. wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz firmy bez upoważnienia IOD;
7. udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej;
8. telefoniczne próby wyłudzenia danych osobowych;
9. kradzież komputerów lub CD, twardych dysków, Pendrive z danymi osobowymi;
10. maile zachęcające do ujawnienia identyfikatora i/lub hasła;
11. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów;
12. hasła do systemów przechowywane są w pobliżu komputera.