5de
kancelaria prawna

Materiały szkoleniowe

z zakresu ochrony danych osobowych ver. 1.0

dla pracowników
Zespołu Opieki Zdrowotnej
w Oleśnie

Podstawy prawne ochrony danych (1)

Ochrona danych osobowych regulowana jest wieloma aktami normatywnymi poczynając od przepisów art. 47 i art. 51 Konstytucji RP.

Inne najważniejsze akty to:

- 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.2016.119.1;
- Ustawa o ochronie danych osobowych;
- Ustawa o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679;
- Kodeks pracy;
- Ustawa o prawach pacjenta i Rzeczniku Praw Pacjenta;
- Ustawa o działalności leczniczej.

5de kancelaria prawna

Podstawy prawne ochrony danych (2)

Bez względu na status (pracowniczy lub inny) osoba mająca dostęp do danych osobowych musi przestrzegać reguł postępowania z danymi osobowymi, które ustalone zostały przez administratora danych (ŚCR). Zawierać je będą wszelkie regulaminy, procedury, instrukcje i inne wewnętrzne regulacje (w tym dobre praktyki) przyjęte i wdrożone przez pracodawcę ustanawiające szczegółowe reguły postępowania w związku z przetwarzaniem danych osobowych.

Pamiętaj:

- To ŚCR, uwzględniając przepisy prawa, określa szczegółowe zasady i procedury postępowania z informacjami podlegającymi ochronie - należy zatem przestrzegać regulaminów, instrukcji i innych poleceń przełożonych !!!
- Każdy z pracowników musi się zapoznać z obowiązującymi regulacjami !!!
- Obowiązek przestrzegania zasad ochrony danych osobowych jest podstawowym obowiązkiem pracowniczym !!!

5de kancelaria prawna

Pojęcie danych

Dane osobowe:

- oznaczają wszelkie 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.

Nie oznacza to, że każda informacja ma samodzielnie identyfikować osobę fizyczną a jedynie to, że ich suma może do tego prowadzić.

Pamiętaj:

- Każda informacja może zostać uznana za dane osobowe, jeśli dołączymy ją do innych danych dotyczących konkretnej osoby fizycznej !!!
- Informacje o konkretnej osobie podlegają ochronie na mocy RODO tylko jeśli osoba ta żyje !!!

5de kancelaria prawna

Przykłady danych osobowych (1)

Standardowo występujący zestaw informacji składający się z danych osobowych zawiera:

- imię i nazwisko
- adres zamieszkania
- PESEL
- funkcję /nazwę stanowiska pracy
- nr telefonu
- i inne dane kontaktowe
- dane o stanie zdrowia

Zestaw ten może składać się z większej lub mniejszej ilości informacji o osobie fizycznej. Ważne jest by pamiętać, że dowolna (wiążąca się w jakikolwiek sposób z tą osobą) informacja dołączona do takiego zestawu automatycznie uzyskuje status danych osobowych.

5de kancelaria prawna

Przykłady danych osobowych (2)

Nie ulega wątpliwości, że status danych osobowych mają obecnie również takie informacje, których powiązanie z konkretną osobą fizyczną może budzić wątpliwości. Są to np.:

- adres e-mail nie zawierający informacji imiennie wskazujących użytkownika;
- niezarejestrowany w bazie administratora nr telefonu;
- informacje identyfikujące urządzenia służące do komunikacji (np. adres IP);
- dane geolokalizacyjne użytkowanych urządzeń (np. dane z GPS dotyczące samochodów, laptopów, telefonów);
- dane z oprogramowania czuwającego nad bezpieczeństwem (informacje z programów antywirusowych);
- dane dotyczące członków rodziny.

5de kancelaria prawna

Przykłady danych osobowych (3)

Pamiętaj:

- Ostateczne uznanie informacji za dane osobowe zależy od analizy stanu faktycznego przeprowadzonej przez administratora (ŚCR) - to on ma pełną wiedzę obejmującą całość procesu przetwarzania tych danych !!!
- Adres poczty elektronicznej należy traktować jako informację, która potencjalnie może być daną osobową, ale z uwzględnieniem wszelkich okoliczności występujących w konkretnym przypadku; podstawowym kryterium ułatwiającym uznanie adresu e-mail za daną osobową będzie w szczególności jego treść (np. zawierająca imię lub skrót imienia i nazwisko). Nie zawsze jednak adres ten prowadzi do identyfikacji osoby fizycznej, może dotyczyć również innych podmiotów nie będących osobami fizycznymi !!!
- Danymi osobowymi pacjenta mogą być również dane kontaktowe osoby uprawnionej do dostępu do dokumentacji medycznej lub informacji o jego stanie zdrowia – ponieważ za pomocą tych danych możemy potencjalnie dotrzeć do samego pacjenta.

5de kancelaria prawna

Przykłady danych osobowych (4)

- Pojęciem danych osobowych obejmujemy również informacje o osobach prowadzących działalność gospodarczą czy informacje o przedstawicielach i pełnomocnikach podmiotów wchodzących w relacje z administratorem danych. Nie jest bowiem istotne w jakiej roli czy charakterze, występują osoby fizyczne.
- Brak możliwości „łatwego" rozpoznania osoby również nie ma większego znaczenia i za dane osobowe uważa się zarejestrowane wizerunki dostępne w ramach monitoringu, obejmujące wizerunek osoby nie będącej pracownikiem np. pacjenta i jego bliskich.

Pamiętaj:

- Używając informacji o przedsiębiorcy będącym osobą fizyczną przetwarzasz dane osobowe !!!
- Jawność i pełna dostępność informacji o osobie fizycznej nie prowadzi do utraty statusu danych osobowych !!!
- Uzyskując z ogólnie dostępnych źródeł informacje kontaktowe prowadzące do osób fizycznych przetwarzasz dane osobowe (np. adres e-mail, numer telefonu)!!!

5de kancelaria prawna

Pojęcie przetwarzania (1)

- Zgodnie z definicją ujętą w RODO pod pojęciem przetwarzania danych kryje się każda operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany.
- Za typowe operacje na danych uznajemy ich 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.
- W pojęciu tym mieszczą się również wszelkie inne działanie bezpośrednio mające lub mogące mieć wpływ na dane np.: przenoszenie i przewożenie fizycznych nośników zawierających dane osobowe (np. dokumenty papierowe, nośniki elektroniczne).

5de kancelaria prawna

Pojęcie przetwarzania (2)

- W konkretnych sytuacjach za przetwarzanie uznaje się również dostęp do oprogramowania (np. w celach serwisowych), umożliwiający ingerencję lub zapoznanie się z danymi oraz serwisowanie sprzętu zawierającego moduły pamięci (które mogą zawierać dane osobowe).

Pojęcie naruszenia ochrony danych

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.

Pamiętaj:

- Jeżeli robisz cokolwiek z użyciem danych osobowych ma miejsce ich przetwarzanie !!!
- Przesyłanie informacji o pacjencie, pracowniku z wykorzystaniem e-mail jest przetwarzaniem danych osobowych !!!
- Dostęp do bazy kontaktów zawierających dane osobowe jest również przykładem przetwarzania danych osobowych !!!
- Wrzucenie jakiegokolwiek dokumentu papierowego zawierającego dane osobowe do kosza na śmieci bez ich uprzedniego zniszczenia będzie naruszeniem zasad ich ochrony !!!
- Przesłanie dokumentacji osobie nieuprawnionej, wysłanie wiadomości mailowej zawierającej dane osobowe do innego odbiorcy niż była ona przeznaczona, przypadkowe lub zamierzone usunięcie danych osobowych pacjentów, pracowników – to są klasyczne przykłady naruszenia ochrony danych !!!

5de kancelaria prawna

Obowiązki Pracownika i Wykonawcy (1)

- Przestrzeganie procedur dostępowych – odpowiednie logowanie, nieujawnianie a tym bardziej celowe przekazywanie indywidualnych danych dostępowych, niepozostawianie informacji dostępowych/kart dostępu bez osobistego (lub regulaminowego) nadzoru;
- Przestrzeganie procedur i instrukcji dot. przetwarzania danych osobowych obowiązujących w ŚCR w szczególności procedur udostępniania, usuwania danych;
- Zakaz używania kart dostępu / identyfikatorów (haseł i loginów) innych użytkowników;
- Zgłaszanie zagubienia kart / podejrzenia dostępu do danych identyfikacyjnych ze strony osób nieuprawnionych;
- Śledzenie komunikatów i uczestnictwo w szkoleniach związanych z bezpieczeństwem informacji;
- Prawidłowe (zgodne z przyjętymi przez pracodawcę) rozliczanie pracy;
- Przetwarzanie danych w zakresie adekwatnym do zakresu obowiązków na stanowisku pracy;
- Odpowiednie, szczególnie uważne zabezpieczenie danych w czasie pracy zdalnej.

5de kancelaria prawna

Obowiązki Pracownika i Wykonawcy (2)

Pamiętaj:

- Obowiązek to nakaz bądź zakaz określonego zachowania się. W obszarze ochrony danych osobowych obowiązki te wynikać będą z sumy wszystkich regulacji przyjętych i wdrożonych przez administratora, którym jest Twój Pracodawca !!!
- Każda próba nielegalnego pozyskania danych, omyłkowego ich udostępnienia, utrata danych musi być natychmiast zgłoszona przełożonemu !!!
- Każde usuniecie danych (w systemie informatycznym, czy w postaci klasycznej) musi być dokonane zgodnie z obowiązującymi procedurami/zasadami !!!

5de kancelaria prawna

Obowiązki Pracownika i Wykonawcy (3)

Przygotowanie i zabezpieczenie pomieszczenia w którym odbywa się przetwarzanie danych osobowych:

- niedopuszczanie osób postronnych;
- niewykonywanie pracy zdalnej w pomieszczeniach ogólnodostępnych i środkach komunikacji zbiorowej;
- niepozostawiane urządzeń służących do pracy bez nadzoru lub odpowiedniego zabezpieczenia (np. wylogowania z systemu operacyjnego;
- przechowywanie nośników informacji (w tym ew. notatek, wydruków itp.) wyłącznie w zabezpieczonych pomieszczeniach/pojemnikach.

Pamiętaj:

Osoba nieuprawniona nie może uzyskać dostępu do danych, które przetwarzasz !!!

Niedopuszczalne jest rejestrowanie/zapisywanie jakichkolwiek danych przez osoby do tego nieuprawnione!!!

Używanie przez osobę nieuprawnioną urządzeń rejestrujących jest zakazane, podstawą tego zakazu jest konieczność ochrony procesu przetwarzania danych!!!

5de kancelaria prawna

Obowiązki Pracownika i Wykonawcy (4)

Przygotowanie i zabezpieczenie urządzeń / transmisji danych:

- korzystanie wyłącznie z bezpiecznych łączy zgodnie z protokołem określonym przez pracodawcę (ogólnodostępne wi-fi itp. są zakazane);
- użytkowanie wydzielonego funkcjonalnie połączenia (innego niż reszta domowników);
- „higiena użytkowania" poczty i komunikatorów: zakaz otwierania załączników, linków itp. od nieautoryzowanych nadawców, potwierdzanie autentyczności poleceń w przypadku treści wywołujących wątpliwości (polecenia niestandardowe, błędy językowe), sprawdzanie danych źródłowych nadawcy komunikatu (w szczególności podgląd pełnego adresu);
- udostępnianie na życzenie pracodawcy urządzeń, na których wykonywana jest praca zdalna, w celu ich odpowiedniego przygotowania i/lub przestrzeganie instrukcji udzielonych w tym zakresie.

5de kancelaria prawna

Obowiązki Pracownika i Wykonawcy (5)

Pamiętaj:

zawsze o wdrożonych przez administratora procedurach i zasadach w zakresie ochrony danych (!!!); ich przestrzeganie jest niezbędne w celu wykazania braku Twojej odpowiedzialności pracowniczej, a nawet karnej !!!

nie zostawiaj dokumentów oraz innych nośników danych, a także włączonego komputera bez nadzoru oraz w sposób umożliwiający zapoznanie się z danymi przez osoby nieuprawnione (!!!)

o ile to możliwe, przenosząc dokumenty również zadbaj oto, aby osoby postronne nie mogły pozyskać jakichkolwiek danych (np. stosuj „ślepe" okładki, teczki, koperty itd. bez opisów odwołujących się do danych osobowych, które będą identyfikowały osobę/osoby fizyczne) (!!!).

.

5de kancelaria prawna

Odpowiedzialność Pracownika i Wykonawcy (6)

- Na podstawie przepisów Kodeksu Pracy w obecnym stanie prawnym administrator danych może żądać odszkodowania od Pracownika za wyrządzoną szkodę z tytułu niewykonania lub nienależytego wykonania obowiązków. Obowiązki te precyzują w zakresie ochrony danych wszelkie dokumenty wewnętrzne związane z ustanowieniem zasad postępowania z danymi.

- Odszkodowanie ustala się w wysokości wyrządzonej szkody, jednak nie może ono przewyższać kwoty trzymiesięcznego wynagrodzenia przysługującego Pracownikowi w dniu wyrządzenia szkody. Wyjątkiem jest sytuacja, gdy Pracownik umyślnie wyrządził szkodę – wówczas obowiązany jest do jej naprawienia w pełnej wysokości oraz naprawienia szkody wyrządzonej przez pracownika. Pracownik ponosi odpowiedzialność za szkodę w granicach rzeczywistej straty poniesionej przez pracodawcę i tylko za normalne następstwa działania lub zaniechania, z którego wynikła szkoda.

5de kancelaria prawna

Odpowiedzialność Pracownika i Wykonawcy (7)

- Należy podkreślić, że przepisy Kodeksu Pracy pozwalają również stosować sankcje dyscyplinarne wobec pracowników, którzy nie przestrzegają zasad RODO (i innych norm ochrony danych osobowych), tym samym naruszając obowiązki pracownicze.

- W zakresie odpowiedzialności wynikającej z Kodeksu Cywilnego Pracownicy na umowach cywilnoprawnych mogą ponosić odpowiedzialność na zasadach ogólnych, tj. za niewykonania lub nienależyte wykonania umowy (art. 471 i nast. KC), odpowiedzialność z tytułu zastrzeżonych w umowie kar umownych, a także odpowiedzialność deliktową (art. 415 i nast. KC).

5de kancelaria prawna

Odpowiedzialność Pracownika i Wykonawcy (8)

- Złamanie zasad wewnętrznych i wykrocznie poza zakres umocowania do przetwarzania nadanego przez administratora (upoważnienia lub innego określenia zakresu dopuszczalnych działań obejmujących przetwarzanie danych) może skutkować odpowiedzialnością karną określoną w ustawie o ochronie danych osobowych (uodo) i Kodeksie karnym.

Odpowiedzialność Pracownika i Wykonawcy (9)

Art. 107 uodo stanowi, że:

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.

Odpowiedzialność Pracownika i Wykonawcy (10)

- Szczególną sytuacją jest ujawnianie danych osobowych, z którymi Pracownik/ Wykonawca zapoznał się w trakcie wykonywania obowiązków, po ustaniu zatrudnienia/zlecenia – dzieje się to w oczywisty sposób wbrew uprawnieniu, gdyż ustaje ono z chwilą rozwiązania umowy.

Pamiętaj:

- O tym czy będziesz mógł uwolnić się od odpowiedzialności decyduje to, czy postępowałeś w zgodzie z obowiązującymi zasadami i procedurami wdrożonymi przez administratora !!!
- Przestrzeganie zasad ochrony danych osobowych jest podstawowym obowiązkiem pracowniczym !!!
- Po zakończeniu zatrudnienia ujawnianie jakichkolwiek danych pozyskanych w czasie jego trwania może stanowić naruszenie przepisów prawa (tajemnica pacjenta trwa również po jego śmierci)!!!

5de kancelaria prawna

Przykłady typowych błędów prowadzących do naruszeń ochrony danych (1)

- Wysłanie e-maila, udzielenie informacji bez sprawdzenia/potwierdzenia tożsamości odbiorcy;
- Wydanie dokumentów/przesyłek z danymi bez sprawdzenia uprawnienia „kuriera”;
- Ujawnianie danych bez wiedzy o uprawnieniach odbiorcy informacji (np. na błędnym domniemaniu posiadania uprawnienia do informowania danych o stanie zdrowia pacjenta pełnoletniego ojcu, matce, bratu);
- Wykorzystywanie danych w celach innych niż te, dla których zostały zgromadzone;
- Brak weryfikacji prawidłowości danych kontaktowych przed ich użyciem (chodzi o weryfikacje zarówno danych otrzymywanych z zewnątrz jak i wpisywanych bezpośrednio przez pracownika – uwaga na systemy automatycznej podpowiedzi treści);

5de kancelaria prawna

Przykłady typowych błędów prowadzących do naruszeń ochrony danych (2)

- Nieautoryzowane zapisywanie danych i ich użytkowanie poza procedurami (np. robienie zdjęć ekranów i ich udostępnianie lub wykorzystanie samodzielne, wysyłanie e-maili z danymi);
- Pozostawianie stanowiska pracy bez dopełnienia procedur wylogowania;
- Ujawnianie danych współpracowników itp. „poza godzinami pracy" na portalach internetowych i innych platformach komunikacyjnych (tweety, zdjęcia, filmiki z miejsca pracy itp.).

Pamiętaj:

- Przed wysłaniem korespondencji elektronicznej sprawdź ponownie prawidłowość adresata (adresatów) !!!
- Nie udzielaj informacji na temat danych osobowych telefonicznie dzwoniącemu (lub temu do kogo dzwonisz), którego identyfikacja budzi wątpliwości !!!
- Zawsze weryfikuj dane kontaktowe !!!
- Nie zamieszczaj danych współpracowników na portalach internetowych i innych platformach komunikacyjnych (tweety, zdjęcia, filmiki z miejsca pracy itp.) !!!

5de kancelaria prawna

Współpraca z osobą odpowiedzialną za ochronę danych osobowych (IOD) (1)

- **IOD to:**
  - o osoba powołana/zatrudniona do pomocy administratorowi przy przestrzeganiu przepisów o ochronie danych osobowych;
- **Współpraca z IOD:**
  - Powiadamianie o istniejących wątpliwościach co do adekwatności istniejących procedur do faktycznych potrzeb;
  - Zgłaszanie zauważonych naruszeń procedur i odbiegającego od standardów funkcjonowania systemów informatycznych (w kontekście przetwarzania danych);
  - Informowanie o incydentach zgodnie z przyjętymi procedurami.

5de kancelaria prawna

Współpraca z osobą odpowiedzialną za ochronę danych osobowych (IOD)(2)

Pamiętaj:

- Każde nieuprawnione lub przypadkowe ujawnienie lub nieuprawniony dostęp do danych osobowych to naruszenie ochrony danych osobowych !!!
- Każde nieuprawnione lub przypadkowe zmodyfikowanie danych osobowych to naruszenie ochrony danych osobowych !!!
- Każdy nieuprawniony lub przypadkowy dostęp do danych osobowych lub ich zniszczenie to naruszenie ochrony danych osobowych !!!
- Jeżeli masz jakiekolwiek wątpliwości związane z czynnościami, które wykonujesz, a które dotyczą danych osobowych skontaktuj się z IOD !!!
- Jeżeli popełnisz błąd, którego skutkiem jest np. przesłanie danych jednej osoby do innej, poinformuj o tym natychmiast IOD !!!
- Jeżeli zgubisz identyfikator, nośnik, laptop lub inny nośnik informacji natychmiast poinformuj o tym IOD !!!

5de kancelaria prawna

Jeśli masz wątpliwości co do treści materiałów …

to dobrze !

Skontaktuj się z przełożonym lub IOD!

Dane kontaktowe Inspektora Ochrony Danych:

dr Tomasz Radziszewski, e-mail: iod@5de.pl, mobile: +48 731 303 621

5de
kancelaria prawna