Zasady ochrony danych osobowych

RODO PORADNIK

Dla pracowników

Zasady ochrony danych osobowych i bezpieczeństwa informacji – co każdy pracownik wiedzieć powinien

Informacje zawarte w poradniku mają na celu przedstawienie w przystępny sposób podstawowej terminologii oraz zasad dotyczących ochrony danych osobowych i bezpieczeństwa informacji. Przestrzeganie wskazanych reguł jest obowiązkiem każdego pracownika lub współpracownika organizacji, mającego lub mogącego mieć do czynienia z danymi osobowymi. Złamanie tych zasad może zostać uznane za ciężkie naruszenie obowiązków pracowniczych lub zobowiązań umownych. Zapoznaj się z nimi, aby wiedzieć, po co i w jaki sposób chronić dane osobowe.

DANE OSOBOWE

– informacje o zidentyfikowanej (np. Jan Nowak, ul. Hoża 5/12, 02-512 Warszawa) lub możliwej do zidentyfikowania osobie fizycznej (np. osoba o numerze PESEL 91121720152); możliwa do zidentyfikowania osoba fizyczna to osoba, której tożsamość można ustalić bezpośrednio lub pośrednio, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, dane o lokalizacji, identyfikator internetowy (adres poczty elektronicznej, nick na forum) lub jeden bądź kilka szczególnych czynników określających fizyczną (np. skan tęczówki oka lub odcisk palca), fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej (np. dyrektor teatru, członek zarządu, radny urzędu gminy).

PRZETWARZANIE DANYCH OSOBOWYCH

– operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany (systemy informatyczne) lub niezautomatyzowany (forma papierowa), w tym przede wszystkim: 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 (np. zapisanie danych na kartce papieru, przechowywanie kwestionariuszy osobowych, archiwizacja formularzy kontaktowych, zapisanie danych na pendrivie, przesłanie kopii umów, wysłanie marketingu elektronicznego).

PRZYKŁADY OPERACJI PRZETWARZANIA:

Zbieranie danych
(np. przez papierowe formularze, przez stronę internetową)

Przeglądanie danych
(np. na komputerze, w archiwum)

Niszczenie danych
(np. w niszczarce, wielokrotne pełne formatowanie dysku)

Ujawnienie danych
(np. poprzez przesłanie e-maila, przesłanie listu wraz z danymi)

Porządkowanie danych
(np. przypisywanie ich do różnych baz danych, porządkowanie danych w kartotekach)

ADMINISTRATOR DANYCH

– osoba fizyczna lub prawna, organ publiczny, jednostka organizacyjna, które samodzielnie lub wspólnie z innymi decydują o celach i sposobach przetwarzania danych osobowych (np. adwokat prowadzący własną kancelarię, spółka z ograniczoną odpowiedzialnością, stowarzyszenie, biblioteka, szkoła lub przedszkole).

PODMIOT PRZETWARZAJĄCY (PROCESOR)

– osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu i na rzecz administratora. Procesorem będzie więc podmiot zewnętrzny, który zgodnie z zawartą z administratorem umową o powierzeniu danych do przetwarzania i tylko w zakresie w niej określonym wspiera administratora w określonych sferach jego działalności, przetwarzając w jego imieniu dane osobowe (np. firma hostingowa, biuro księgowe,

firmy drukujące lub obsługujące korespondencję otrzymywaną od klientów, firmy archiwizujące dokumenty, firmy zajmujące się badaniami opinii klientów, partnerzy świadczący usługi techniczne, takie jak rozwijanie i utrzymywanie systemów informatycznych i serwisów internetowych).

WIĘCEJ

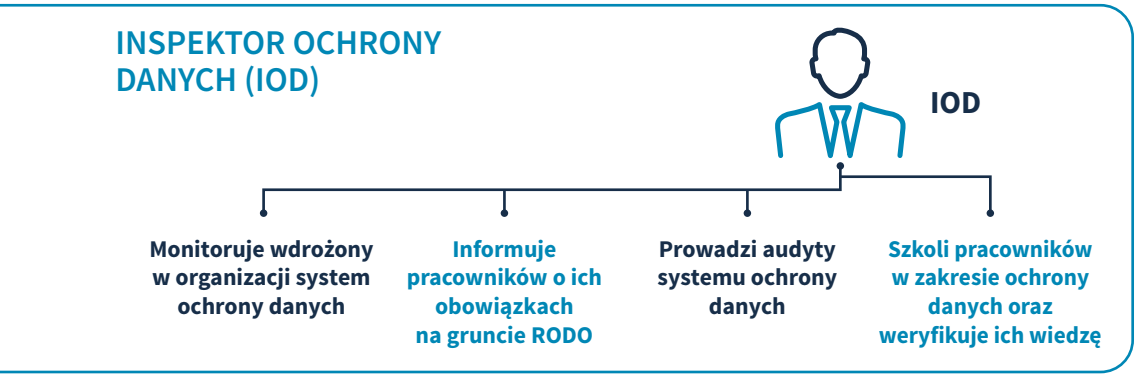
PODMIOT PRZETWARZAJĄCY

Przykłady podmiotów przetwarzających

- **Firma obsługująca księgowość**
- **Firma obsługująca kadry i payroll**
- **Firma niszcząca dokumenty i sprzęt**
- **Firma świadcząca usługi zewnętrznego archiwum**
- **Firma świadcząca usługi z zakresu IT**

INSPEKTOR OCHRONY DANYCH (IOD)

– osoba wyznaczona przez administratora danych lub podmiot przetwarzający, która monitoruje i weryfikuje przestrzeganie przepisów o ochronie danych osobowych oraz doradza w tym zakresie i wydaje odpowiednie rekomendacje.



ORGAN NADZORCZY (PREZES URZĘDU OCHRONY DANYCH OSOBOWYCH – PREZES UODO)

– niezależny organ publiczny odpowiedzialny za monitorowanie stosowania przepisów o ochronie danych osobowych.

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH

– upoważnienie nadawane przez administratora danych lub podmiot przetwarzający, wskazujące z imienia i nazwiska osobę, która ma prawo przetwarzać dane w zakresie wskazanym w tym upoważnieniu.

Znajomość powyższej terminologii i umiejętność jednoznacznego identyfikowania poszczególnych funkcji w organizacji są kluczowe ze względu na konieczność nie tylko przestrzegania zasad zawartych w dokumentacji przetwarzania danych, lecz także wykazania się tym podczas ewentualnej kontroli organu nadzorczego – Prezesa UODO.

Zasady przetwarzania danych

Poniżej przedstawiamy najważniejsze zasady, których przestrzeganie pozwala na zgodne z prawem przetwarzanie danych osobowych.

ZASADA LEGALNOŚCI ORAZ PRZEJRZYSTOŚCI

– przetwarzanie danych osobowych musi odbywać się zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą. Musi istnieć podstawa prawna przetwarzania, jak zgoda osoby, której dane dotyczą, lub niezbędność przetwarzania danych do wykonania umowy (np. podanie danych przez pracownika jest niezbędne do wykonania umowy o pracę, w tym wypłacenia należnego mu wynagrodzenia). Podstawy przetwarzania są określone w art. 6 i 9 RODO.

ZASADA CELOWOŚCI

– cel przetwarzania danych osobowych musi być z góry określony, a informacja ta musi zostać przekazana osobie, której dane dotyczą. Aby dane mogły być przetwarzane, musi istnieć konkretny, wyraźny i prawnie uzasadniony cel. Przetwarzanie danych w sposób niezgodny z ustalonymi celami jest zakazane.

ZASADA ADEKWATNOŚCI (MINIMALIZACJI DANYCH)

– administrator powinien przetwarzać tylko te dane, które są niezbędne ze względu na cel ich zbierania, np. nieadekwatne będzie pozyskiwanie kserokopii dowodu osobistego w trakcie zawierania umowy z peratorem-telekomunikacyjnym.

ZASADA MERYTORYCZNEJ POPRAWNOŚCI

– dane osobowe muszą być prawdziwe, kompletne i aktualne ze względu na cel, jakiemu mają służyć. Nie można zbierać danych osobowych ze źródeł nieznanego pochodzenia. Należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.

ZASADA OGRANICZENIA PRZECHOWYWANIA

– dane osobowe mogą być przechowywane w formie umożliwiającej identyfikację osoby, której dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te zostały pozyskane (np. gdy celem zbierania CV była konkretna rekrutacja, administrator nie może przechowywać CV kandydatów na potrzeby przyszłych rekrutacji

bez dodatkowej zgody – powinien je usunąć do 3 miesięcy po zakończeniu rekrutacji).

ZASADA INTEGRALNOŚCI I POUFNOŚCI DANYCH

– przetwarzanie danych powinno następować w sposób zapewniający im odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych po uwzględnieniu ryzyk.

ZASADA ROZLICZALNOŚCI

– administrator jest odpowiedzialny za przestrzeganie przepisów o ochronie danych osobowych i musi być w stanie wykazać, że stosuje się do nich (np. w razie kontroli powinien wykazać, że realizuje względem osób, których dane dotyczą, obowiązek informacyjny lub stosuje odpowiednie środki techniczne i organizacyjne zabezpieczające przed nieuprawnionym dostępem do danych ze strony osób trzecich).

WIĘCEJ

Zasady i procedury bezpieczeństwa danych

PROCEDURY I ZASADY ZABEZPIECZENIA DANYCH JAKIE POWINIEN ZNAĆ PRACOWNIK

Polityka ochrony danych

Zasady bezpieczeństwa:
- czyste biurko
- czysty ekran
- czysty wydruk

Procedura niszczenia danych

Procedura korzystania z internetu, poczty elektronicznej oraz urządzeń moblinych

Procedura zgłaszania naruszeń

Poniżej przedstawiamy najważniejsze zasady i kluczowe procedury bezpieczeństwa danych osobowych.

ZASADA „CZYSTEGO" BIURKA

– należy pamiętać o konieczności przechowywania wszelkich nośników danych osobowych (np. dokumentów) poza zasięgiem wzroku i dłoni osób postronnych, a także o przechowywaniu takich nośników pod kluczem.

ZASADA „CZYSTEGO" EKRANU

– należy pamiętać o konieczności blokowania komputerów przed każdorazowym, nawet chwilowym opuszczeniem stanowiska pracy (np. skrót klawiszowy WIN + L). Dodatkowo należy uniemożliwić osobom nieupoważnionym wgląd w treści wyświetlane na monitorach – choćby przez odpowiednie ustawienie ekranu lub stosowanie filtrów prywatyzujących.

ZASADA „CZYSTEGO" (POUFNEGO) DRUKU

– należy pamiętać o konieczności odbierania z urządzeń drukujących wszelkich dokumentów niezwłocznie po ich wydrukowaniu.

POLITYKA OCHRONY DANYCH

- w każdej organizacji funkcjonuje dokument opisujący kluczowe kwestie wiążące się z ochroną danych osobowych. Pracownicy właśnie tam znajdą najważniejsze informacje w przedmiocie tego jak chronić dane osobowe.

PROCEDURA ZGŁASZANIA NARUSZEŃ

- należy pamiętać o konieczności zgłaszania wszelkiego rodzaju naruszeń ochrony danych osobowych. Pracownik musi szybko zareagować w sytuacji wykrycia zagrożenia dla bezpieczeństwa danych lub w sytuacji wystąpienia naruszenia ochrony danych osobowych.

PROCEDURA NISZCZENIA

– należy pamiętać o konieczności niszczenia dokumentacji zawierającej dane osobowe,

z wykorzystaniem niszczarek lub pojemników do utylizacji dokumentów.

PROCEDURA KORZYSTANIA Z URZĄDZEŃ MOBILNYCH

– należy pamiętać o szczególnie silnym zabezpieczaniu urządzeń wynoszonych poza obszar pracy (obszar przetwarzania danych), w tym o stosowaniu szyfrowania nośników takich urządzeń. Jeśli nie masz pewności, czy zabezpieczenie zostało wdrożone, zgłoś się do działu IT.

PROCEDURA KORZYSTANIA Z INTERNETU

– należy unikać zapisywania haseł w przeglądarkach internetowych. Jeśli mimo to zdecydujesz się na takie zachowanie, upewnij się, czy w ustawieniach przeglądarki dostęp do zapisanych haseł jest zabezpieczony dodatkowym hasłem głównym. W przeciwnym wypadku osoba nieuprawniona może pozyskać wszystkie dane logowania.

PROCEDURA KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

– podczas wysyłania wiadomości e-mail należy pamiętać o stosowaniu kopii ukrytej,

w szczególności gdy dochodzi do masowej wysyłki korespondencji. Ponadto nie wolno otwierać załączników z wiadomości od nieznanych adresatów.

PROCEDURA KORZYSTANIA Z ZASOBÓW ORGANIZACJI

– istotne dokumenty w formie elektronicznej, w tym zawierające dane osobowe, należy przechowywać na udostępnionych zasobach sieciowych. Jeżeli zapisujesz je na dysku lokalnym, musisz liczyć się z tym, że w razie kradzieży, zgubienia, uszkodzenia lub zainfekowania urządzenia ich odzyskanie może być już niemożliwe.

Najczęściej występujące zagrożenia

Poniżej przedstawiamy najczęściej występujące sytuacje, które zagrażają bezpieczeństwu danych osobowych:

opuszczanie stanowiska pracy i pozostawianie aplikacji lub systemu operacyjnego bez wylogowania się z nich – umożliwia to osobie nieuprawnionej dostęp do bazy danych osobowych,

umyślne dopuszczanie do korzystania z systemu operacyjnego lub aplikacji umożliwiających dostęp do bazy danych osobowych przez kogokolwiek innego niż osoba, której przydzielono identyfikator,

pozostawianie w miejscu widocznym lub oczywistym zapisanego hasła dostępu do bazy danych osobowych lub sieci, jak również jego współdzielenie z osobami trzecimi,

przechowywanie dokumentów niewłaściwie zabezpieczonych przed dostępem osób nieupoważnionych w zasięgu ich wzroku lub dłoni,

wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie do zwykłych śmietników – niekorzystanie z niszczarek,

dopuszczanie, aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe – niezapewnienie polityki czystego ekranu,

sporządzanie kopii danych na nośnikach danych w sytuacjach nieprzewidzianych procedurą – nieautoryzowane wynoszenie danych osobowych,

wpuszczanie do pomieszczeń osób nieznanych i dopuszczanie do ich kontaktu ze sprzętem komputerowym – pozostawianie osób nieupoważnionych bez nadzoru,

otwieranie poczty elektronicznej pochodzącej od nieznanych nadawców, a w szczególności otwieranie załączników,

korzystanie z publicznie dostępnych sieci Wi-Fi, które nie mają żadnej autoryzacji – brak hasła,

wysyłanie mailingu masowego z wpisaniem adresów w pole DO lub DW zamiast UDW.

W razie wystąpienia któregokolwiek z powyższych zdarzeń należy niezwłocznie skontaktować się z przełożonym, IOD lub z najwyższym kierownictwem organizacji.

WIĘCEJ

Postępowanie w razie wystąpienia zagrożenia

WIĘCEJ

Poniżej przedstawiamy kroki jakie należy podjąć w razie wykrycia zagrożenia bezpieczeństwa danych osobowych lub wystąpienia incydentu.

ZABEZPIECZENIE DANYCH OSOBOWYCH

Jeżeli istnieje możliwość zabezpiecz dane osobowe przed ich utratą, zniszczeniem itd. Przykład – dochodzi do ataku z zewnątrz na zasoby znajdujące się na komputerze pracownika, należy w pierwszej kolejności odłączyć taką stacje roboczą od sieci a następnie wyłączyć komputer.

POWIADOMIENIE IOD, BEZPOŚREDNIEGO PRZEŁOŻONEGO

Każde niepokojące zdarzenie, którego przedmiotem są dane osobowe należy niezwłocznie zgłosić do wyznaczonego w organizacji IOD lub bezpośredniemu przełożonemu. Osoby te muszą bowiem podjąć dalsze kroki, takie jak przygotowanie wewnętrznej dokumentacji dotyczącej naruszenia oraz zbadanie czy dane zdarzenie podlega zgłoszeniu do Prezesa UODO jako naruszenie ochrony danych.

PODJĘCIE ŚRODKÓW MINIMALIZUJĄCYCH ROZMIARY NARUSZENIA

Gdy dochodzi do naruszenia, pracownik musi podjąć wszelkie możliwe kroki, które pozwolą na minimalizację rozmiarów naruszenia.

Przykład - Jeżeli dochodzi do zalania archiwum należy zabezpieczyć dane osobowe, które uległy zalaniu w celu minimalizacji skutków zdarzenia oraz szybko zabezpieczyć dane, które nie uległy jeszcze zalaniu tak aby skala incydentu nie rosła.

SPORZĄDZENIE DOKUMENTACJI

Pracownik w miarę możliwości powinien współpracować z IOD i przełożonym w celu udokumentowania okoliczności zdarzenia. Sporządzenie wewnętrznej dokumentacji jest bowiem obowiązkiem płynącym bezpośrednio z przepisów RODO.

ZASTOSOWANIE DZIAŁAŃ ZAPOBIEGAWCZYCH

Z każdego incydentu z danymi osobowymi powinny zostać wyciągnięte wnioski w postaci działań mających na celu elimina-

cję powtórzenia się sytuacji w przyszłości. Przykład: wprowadzenie czujników zalania w archiwum, wdrożenie odpowiednich zabezpieczeń na komputerach w celu eliminacji ataków z zewnątrz itd.

Raportowanie naruszeń

W przypadku incydentu ochrony danych niezwykle ważne jest dynamiczne działanie. Administrator powinien ustalić jego przyczyny, zasięg oraz potencjalne konsekwencje i podjąć decyzję, czy należy zawiadomić Prezesa UODO i osoby, których dane zostały ujawnione.

Incydent podlega zgłoszeniu do Prezesa UODO, gdy może skutkować ryzykiem naruszenia praw i wolności osób, np. jeśli naruszenie może prowadzić do kradzieży lub fałszowania tożsamości, straty finansowej, naruszenia dobrego imienia czy też naruszenia tajemnic prawnie chronionych. W takim przypadku administrator musi zgłosić naruszenie do Prezesa UODO nie później niż 72 godziny po stwierdzeniu (wykryciu) incydentu.

Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia o takim zdarzeniu osobę, której dane dotyczą.

Decyzję o zgłoszeniu naruszenia do Prezesa UODO w imieniu administratora danych podejmuje najwyższe kierownictwo (np. zarząd). Inspektor ochrony danych (IOD) pełni w tym zakresie funkcję doradczą.

WIĘCEJ

Kontakt w razie naruszenia

.....

Chcesz wiedzieć więcej?

RODO migawka
Cykl bezpłatnych mikroszkoleń
ODO24.pl/RODO-migawka

Oglądaj nas
Na naszym kanale na YouTube
youtube.com/ODO24pl

Pomoc ODO 24
Bezpłatne porady
ODO24.pl/Pomoc

Biuletyn informacyjny
Tylko to, co najważniejsze
ODO24./Biuletyn

Ochrona Danych Osobowych

BEZPIECZEŃSTWO INFORMACJI

Audyt zgodności

Wykonujemy pełny audyt zgodności z RODO. Badamy zarówno bezpieczeństwo urządzeń, systemów, sieci i aplikacji, jak i poprawność klauzul, regulaminów oraz rejestrów. Doradzamy, jak praktycznie wdrożyć nasze zalecenia.

Szkolenia otwarte

Dzielimy się wiedzą, pomagamy w zdobyciu umiejętności i wyposażamy w narzędzia, które umożliwią Państwu skuteczne wykonywanie obowiązków związanych z ochroną danych osobowych.

DPIA i analiza ryzyka

Analizę ryzyka i DPIA rozumiemy jako fundament RODO – sposób na racjonalizację kosztów ochrony danych oraz troskę o prywatność osób, których dane Państwo przetwarzają.

Szkolenia zamknięte

Dostosowujemy je do potrzeb organizacji oraz specyfiki branży, w której działa. Stawiamy na praktykę – Państwa pracownicy nauczą się wykorzystywać wiedzę o RODO w swojej codziennej pracy.

Wdrożenie RODO

Wypełniamy „neutralne" technologicznie RODO. Pomagamy dostosować: procesy biznesowe (np. marketing, rekrutacja), środowisko teleinformatyczne, dokumentację ochrony danych.

E-learning

Nasza platforma pozwala w krótkim czasie (nawet w największej organizacji) przeszkolić personel oraz zweryfikować nabytą wiedzę. Minimalizujemy w ten sposób najczęstszą przyczynę incydentów – nieświadomość pracowników.

Przejęcie funkcji IOD

Pełniąc funkcję IOD, wspomagamy i nadzorujemy organizację w utrzymaniu zgodności z RODO. Działamy szybko i efektywnie dzięki doświadczonym ekspertom z obszaru prawa, IT oraz zarządzania ryzykiem.

Narzędzia

Dostarczamy rozwiązania pozwalające kontrolować przepływ danych w organizacji, w tym prowadzić niezbędne rejestry oraz zarządzać szkoleniami, incydentami, upoważnieniami etc.

Bieżące wsparcie

Dzięki dostarczanym przez nas narzędziom oraz wiedzy jesteśmy w stanie przyczynić się do monitorowania i rozwoju funkcjonującego u Państwa systemu ochrony danych osobowych.

Usługi powiązane

Pomoc w razie kontroli UODO, wsparcie we wdrożeniu systemu ISO 27001, ISO 20000, ISO 22301, a także dyrektywy NIS (tzw. cyberustawy).

Jedna specjalizacja

SZEROKA PERSPEKTYWA

- Przepisy prawa
- Bezpieczeństwo sieci i systemów IT
- Zarządzanie ryzykiem
- Bezpieczeństwo fizyczne
- Wiedza i świadomość personelu

ODO24.pl
tel. 22 740 99 00