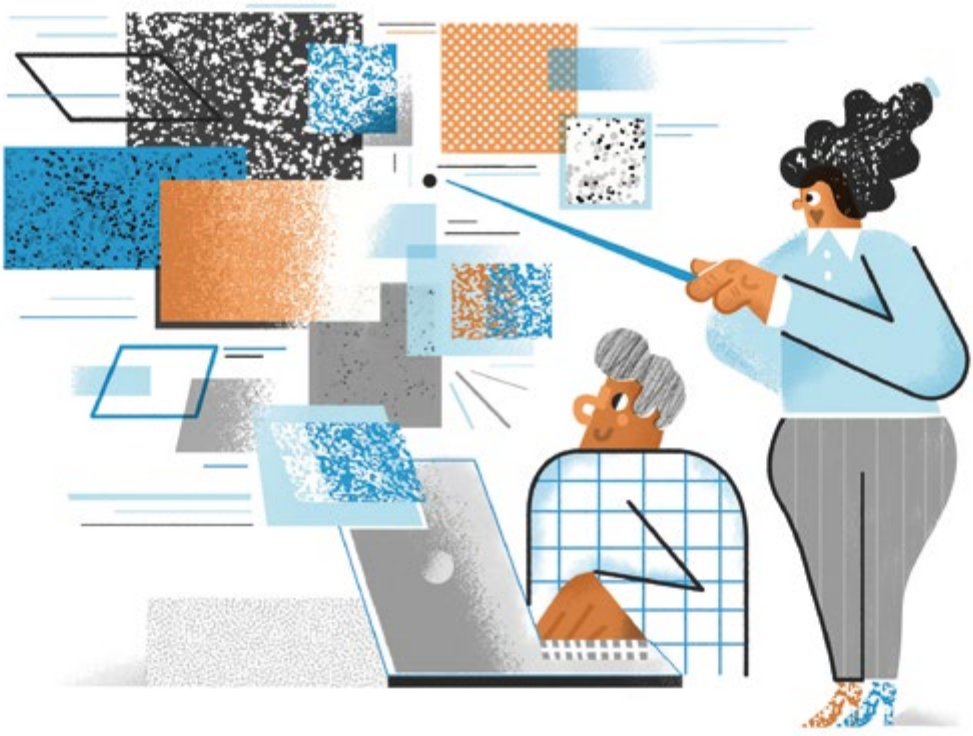
Zasady ochrony danych osobowych



Co każdy pracownik wiedzieć powinien

Zasady ochrony danych osobowych i bezpieczeństwa informacji. Co każdy pracownik wiedzieć powinien.

Poniższe informacje mają na celu przedstawienie w przystępny sposób podstawowej terminologii oraz zasad ochrony danych osobowych i bezpieczeństwa informacji. Przestrzeganie poniższych reguł jest obowiązkiem każdego pracownika lub współpracownika Twojej organizacji, mającego lub mogącego mieć do czynienia z danymi osobowymi. Naruszenie poniższych 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 - oznaczają 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 - oznacza operację 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).

Administrator danych - rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę organizacyjną, 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) - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę 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 (np. rozwijanie i utrzymywanie systemów informatycznych i serwisów internetowych).

Inspektor ochrony danych (IOD) – oznacza osobę wyznaczoną przez administratora danych lub podmiot przetwarzający, która monitoruje i weryfikuje zakres przestrzegania przepisów o ochronie danych osobowych oraz doradza w tym zakresie i wydaje odpowiednie rekomendacje.

Organ nadzorczy (Prezes Urzędu Ochrony Danych Osobowych - PUODO) – niezależny organ publiczny odpowiedzialny za monitorowanie stosowania przepisów o ochronie danych osobowych.

Upoważnienie do przetwarzania danych - rozumie się przez to 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 jednoznaczna identyfikacja poszczególnych funkcji w organizacji są kluczowe, ze względu na konieczność przestrzegania zasad zawartych w dokumentacji przetwarzania danych oraz na ewentualność kontroli organu nadzorczego - Prezesa UODO.

Obowiązkowe zasady postępowania (nakazy)

Poniżej przedstawiamy najważniejsze zasady mające, na celu 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 np. 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 zostały określone w art. 6 i 9 RODO.

Zasada celowości - cel przetwarzania danych osobowych musi być z góry określony i 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 operatorem 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 dane 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 powinien przechowywać CV kandydatów na potrzeby przyszłych rekrutacji bez dodatkowej zgody, oraz 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 się do nich stosuje (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).

Polityka czystego biurka – należy pamiętać o konieczności przechowywania wszelkich nośników danych osobowych (np. dokumentów) poza zasięg wzroku i zasięg dłoni osób postronnych, a także o przechowywaniu ich pod kluczem.

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

Polityka czystego druku – należy pamiętać o konieczności odbierania wszelkich wydruków z urządzeń drukujących niezwłocznie po ich wydrukowaniu.

Procedura niszczenia – należy pamiętać o konieczności niszczenia dokumentów zawierających dane osobowe z wykorzystaniem niszczarek lub pojemników do utylizacji dokumentacji zawierającej dane osobowe.

Procedura korzystania z urządzeń mobilnych – należy pamiętać o konieczności zabezpieczania sprzętu informatycznego (laptopy, smartfony, tablety, pendrive'y) przed wyniesieniem ich poza obszar pracy (obszar przetwarzania danych) – hasłem, PINem, przy zastosowaniu technologii biometrycznych oraz szyfrowaniu zawartych na nich danych.

Procedura korzystania z Internetu – należy pamiętać o zakazie stosowania zapamiętywania haseł w przeglądarkach internetowych oraz historii wyszukiwania – okresowo należy czyścić historię przeglądania lub wyłączyć jej zapamiętywanie.

Procedura korzystania z poczty elektronicznej – należy pamiętać o weryfikacji adresów mailowych w procesie wysyłania tak, by adresacja była prawidłowa – w szczególności należy weryfikować opcje kopia ukryta/kopia jawna. Dodatkowo nie wolno korzystać z odnośników znajdujących się w mailach nieznanego pochodzenia.

Najczęściej występujące zagrożenia

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

Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji lub systemu operacyjnego, umożliwiające dostęp do bazy danych osobowych osobie nieuprawnionej.

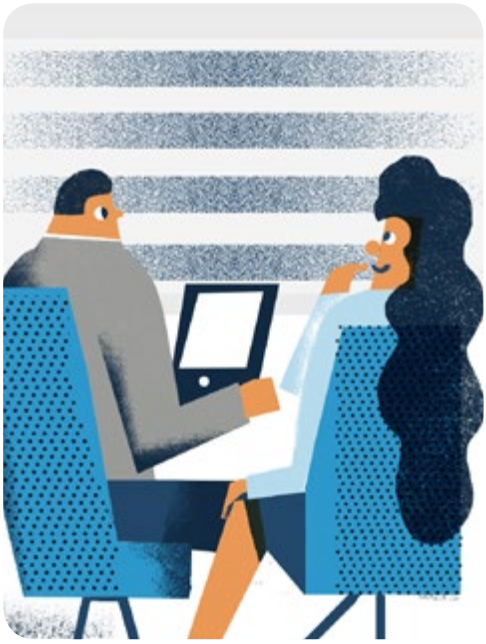
Dopuszczenie do korzystania z systemu operacyjnego lub aplikacji umożliwiających dostęp do bazy danych osobowych przez jakiekolwiek osoby inne niż osoba, której identyfikator został przydzielony.

Pozostawienie 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 do zwykłych śmietników w stopniu zniszczenia umożliwiającym ich odczytanie – 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 załączników.

Korzystanie z publicznie dostępnych sieci Wi-Fi, które nie posiadają żadnej autoryzacji – brak hasła.

Wysłanie 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.

Postępowanie w razie wystąpienia zagrożenia

Poniżej przedstawiamy sposoby postępowania w razie wykrycia zagrożenia bezpieczeństwa danych osobowych lub wystąpienia incydentu.

Należy zabezpieczyć dane osobowe
– jeżeli zdarzenie stwarza taką możliwość.

Należy niezwłocznie zgłosić zdarzenie
IOD, bezpośredniemu przełożonemu lub najwyższemu kierownictwu.

Należy ustalić okoliczności naruszenia
ochrony danych osobowych.

Należy sporządzić dokumentację
naruszenia (notatkę).

Należy zastosować działania zapobiegawcze,
by nie doszło ponownie do zdarzenia.

Należy współpracować z IOD
lub przedstawicielami organu nadzorczego.

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 go zgłaszać do Prezesa Urzędu Ochrony Danych Osobowych i osób, których dane zostały ujawnione.

Incydent podlega zgłoszeniu do Prezesa Urzędu, 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 naruszeniu osobę, której dane dotyczą.

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

Kontakt w razie incydentu

.....