

SZKOLENIE W SYSTEMIE SAMOKSZTAŁCENIA KIEROWANEGO Z ZAKRESU OCHRONY DANYCH OSOBOWYCH

RODO

CZĘŚĆ 4

MODUŁ 4

**Naruszenie ochrony danych - jak powinien postąpić
pracownik?**

INFORMACJE OD INSPEKTORA OCHRONY DANYCH!!!!

Zaprezentowane materiały mają na celu uczulenie pracowników na kwestie związane z bezpieczeństwem przetwarzania danych osobowych. Do prezentacji dołączony został quiz sprawdzający wiedzę pracowników.

ZAPRASZAM JEDNOCZEŚNIE DO KONTAKTU

iodo@iodo.kutno.pl

Paweł Łuczak: Inspektor Ochrony Danych

Podstawa prawna

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (Dz. Urz. UE. L Nr 119, str. 1)- tzw. RODO

- Nowe przepisy zaczęły obowiązywać od 25 maja 2018r.

Wstęp

Administrator danych osobowych jest obowiązany zapewnić aby proces ich przetwarzania był realizowany w warunkach zapewniających właściwy poziom bezpieczeństwa.

Przyjęcie właściwej procedury na wypadek naruszenia ochrony danych osobowych pozwala na sprawne podjęcie działań mając świadomość, że żaden z przyjętych systemów ochrony danych nie jest w 100% skuteczny.

Pracownicy mają obowiązek stosowania przyjętej procedury.

Naruszenie ochrony danych osobowych

Żeby zaistniało naruszenie w zakresie ochrony danych powinny być spełnione łącznie **trzy przesłanki:**

1

Naruszenie dotyczy danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych przez podmiot, którego dotyczy naruszenie,

2

Skutkiem naruszenia jest zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych,

3

Naruszenie jest konsekwencją złamania zasad bezpieczeństwa danych.

Przykładowe naruszenia 1/2

Kiedy dochodzi do naruszeń?

W następujących sytuacjach:

- ślady na drzwiach, oknach i szafach wskazują na próbę włamania,
- zniszczenie dokumentacji zawierającej dane osobowe bez użycia niszczarki,
- fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie,
- otwarte drzwi do pomieszczeń, szaf, w których przechowywane są dane osobowe,
- ustawienie monitorów pozwalające na wgląd osób postronnych w dane osobowe,
- wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz firmy bez upoważnienia inspektora ochrony danych,

Przykładowe naruszenia 2/2

Kiedy dochodzi do naruszeń?

W następujących sytuacjach:

- udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej,
- telefoniczne próby wyłudzenia danych osobowych,
- kradzież komputerów lub CD, twardego dysku, pendrive'a z danymi osobowymi,
- e-maile zachęcające do ujawnienia identyfikatora i/lub hasła,
- pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów,
- przechowywanie haseł do systemów w pobliżu komputera.

Reakcja pracownika

Jak powinien **postąpić pracownik**, gdy stwierdzi naruszenia lub choćby poweźmie przypuszczenie, że doszło do naruszenia?

Konkretne działania zależą od przyjętej u danego administratora **procedury postępowania na wypadek naruszeń**.

Procedura jest również elementem wewnątrzzakładowego prawa pracy, dlatego **wszyscy pracownicy mają obowiązek jej przestrzegania** (chyba że sama procedura stanowi inaczej).

Wprowadzenie procedury nie musi być uzgadniane z pracownikami ani opiniowane przez nich.

Reakcja pracownika

Każdy pracownik, który **stwierdzi lub nawet podejrzewa naruszenie ochrony danych osobowych**, ma obowiązek niezwłocznie zgłosić to bezpośredniemu przełożonemu.

Naruszenie należy zgłosić natychmiast, ponieważ administrator ma jedynie 72 godziny na zgłoszenie naruszenia do UODO.

Reakcja pracownika

Osoby odpowiedzialne za funkcjonowanie systemów informatycznych, w ramach których przetwarzane są dane osobowe, mają obowiązek niezwłocznego informowania inspektora ochrony danych **o każdych nieprawidłowościach w pracy nadzorowanych urządzeń** które mogą być przyczyną lub skutkiem incydentu w zakresie ochrony danych osobowych.

Reakcja pracownika

Pracownik, który stwierdzi fakt naruszenia lub podejrzenia naruszenia danych osobowych ma obowiązek:

- podjąć **czynności niezbędne do powstrzymania skutków naruszenia ochrony,**
- **zabezpieczyć dowody** umożliwiające ustalenie przyczyn oraz skutków naruszenia.

Reakcja pracownika

Bezpośredni przełożony, który otrzymał informację o naruszeniu, musi niezwłocznie zawiadomić o tym naruszeniu:

- **inspektora ochrony danych,**
- w razie braku IOD – **osobę reprezentującą administratora danych osobowych** (np. Dyrektora).

Zgłaszanie naruszeń na zewnątrz i ich dokumentowanie

Pracodawca może sędować na pracowników obowiązki związane z naruszeniem, a wynikające z RODO:

zgłoszenie w imieniu administratora naruszenia do UODO, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia (zgłoszenia nie dokonuje się, gdy jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych); do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia (art. 33 ust. 1 RODO),

zawiadomienie podmiotu danych o naruszeniu, bez zbędnej zwłoki – jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych (art. 34 ust. 1 RODO),

wpisanie naruszenia do **rejestru naruszeń**, w tym wskazanie działań zaradczych (art. 33 ust. 5 RODO).

Konsekwencje uchybień pracownika

- Odpowiedzialność porządkowa
- Naruszenie procedury postępowania na wypadek naruszeń jest uchybieniem porządku pracy.
- Pracownik może otrzymać karę porządkową **upomnienia lub nagany** (z wpisem do akt osobowych)
- Wpływ na zastosowanie i wymiar kary będzie miało wystąpienie pracownika.
- Kara porządkowa może zostać nałożona za samo nieprzestrzeganie procedury, nawet jeżeli nie dojdzie do naruszenia ochrony danych.

Konsekwencje uchybień pracownika

Odpowiedzialność materialna

Może powstać, gdy pracodawca w wyniku zaniechań pracownika poniesie odpowiedzialność finansową (np. zostanie nałożona na niego kara przez Prezesa UODO).

Pracownik może ponieść odpowiedzialność odszkodowawczą względem pracodawcy - do wysokości **3-miesięcznej pensji** (limit nie dotyczy naruszeń umyślnych)

Pracodawca może dochodzić odszkodowania na drodze sądowej.

Konsekwencje uchybień pracownika

Zwolnienie dyscyplinarne

Za szczególnie rażące uchybienia (ciężkie naruszenie podstawowych obowiązków pracowniczych z pracownikiem może zostać rozwiązany stosunek pracy **bez wypowiedzenia**).

Przykład: całkowite zaniechanie poinformowania o ewidentnym i poważnym przypadku naruszenia ochrony danych (np. włamaniu do miejsca, w którym przechowywane są dokumenty zawierające dane) bądź umyślne spowodowanie wycieku danych (np. udostępnienie danych szczególnej kategorii osobie trzeciej).

Rozwiązanie nastąpi w ciągu miesiąca od dnia stwierdzenia naruszenia

SERDECZNIE DZIĘKUJĘ ZA UDZIAŁ W
SZKOLENIU.

ZAPRASZAM DO ROZWIĄZANIA TESTU

W KAŻDYM PYTANIU TYLKO JEDNA ODPOWIEDŹ PRAWIDŁOWA!!!!

BARDZO PROSZĘ W PRZYPADKU JAKICHKOLWIEK PYTAŃ
O KONTAKT:

iodo@iodo.kutno.pl

Paweł Łuczak: Inspektor Ochrony Danych

TEST WIEDZY

1.	Dokumentacja zawierająca dane osobowe została wyrzucona na śmieci. Co powinien zrobić pracownik, który to zauważył?
A.	Niezwłocznie zawiadomić bezpośredniego przełożonego, zgodnie z procedurą obowiązującą w zakładzie pracy.
B.	Zawiadomić bezpośredniego przełożonego, zgodnie z procedurą obowiązującą w zakładzie pracy - w ciągu 72 godzin.
C.	Nie musi podejmować żadnych działań.

TEST WIEDZY

2.	Procedura postępowania na wypadek naruszeń ochrony danych osobowych obowiązuje:
A.	jeśli została opracowana w danym zakładzie pracy.
B.	jeśli została opracowana w danym zakładzie pracy, a wszyscy pracownicy wyrazili zgodę na jej wprowadzenie.
C.	jeśli została opracowana w danym zakładzie pracy, a ogół pracowników zaopiniował jej wprowadzenie.

TEST WIEDZY

3.	Czy pracownik może otrzymać karę porządkową za nieprzestrzeganie procedury postępowania na wypadek naruszeń ochrony danych osobowych?
A.	Tak.
B.	Tak, ale nie za samo nieprzestrzeganie procedury, lecz jeśli wskutek jej nieprzestrzegania doszło do naruszenia ochrony danych.
C.	Tak, i to nawet wówczas, gdy mimo jej nieprzestrzegania nie doszło do naruszenia ochrony danych.

TEST WIEDZY

4.	Czy pracownik ma obowiązek wpisywania danego naruszenia ochrony danych do rejestru naruszeń?
A.	Nie.
B.	Tak, jeżeli taki obowiązek służbowy przydzielili mu pracodawca.
C.	Tak, w każdym przypadku, gdy zauważy, że doszło do naruszenia.

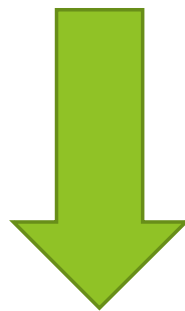
TEST WIEDZY

5.	W przypadku, gdy w wyniku nieumyślnego błędu pracownika UODO nałoży karę na pracodawcę, pracownik:
A.	nie powinien ponosić odpowiedzialności odszkodowawczej.
B.	może ponieść odpowiedzialność odszkodowawczą do wysokości 3-miesięcznej pensji.
C.	może ponieść odpowiedzialność odszkodowawczą w nieograniczonej wysokości.

GRATULUJĘ!!!!



PONIŻEJ PODAJĘ ODPOWIEDZI
ZAPRASZAM DO SAMOOCENY



ODPOWIEDZI

1.	A
2.	A
3.	C
4.	B
5.	C