SZKOLENIE W SYSTEMIE SAMOKSZTAŁCENIA KIEROWANEGO Z ZAKRESU OCHRONY DANYCH OSOBOWYCH

RODO

CZĘŚĆ 3

MODUŁ 3

Bezpieczeństwo danych przede wszystkim - jakie środki ochrony powinni stosować pracownicy?

INFORMACJE OD INSPEKTORA OCHRONY DANYCH!!!!!

Zaprezentowane materiały mają na celu uczulenie pracowników na kwestie związane z bezpieczeństwem przetwarzania danych osobowych. W szkoleniu przedstawiono środki, jakie mogą służyć bezpieczeństwu przetwarzanych danych, przykładowe naruszenia bezpieczeństwa i konsekwencje, jakie mogą grozić za to pracownikom. 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

Bezpieczeństwo danych osobowych oznacza przede wszystkim ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem.

Pracodawca wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku. RODO wskazuje m.in. na:

pseudonimizację i szyfrowanie danych osobowych;

zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;

zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;

regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

To jednak nie jedyne możliwe środki bezpieczeństwa.

Rodzaje środków bezpieczeństwa

O tym, jakie środki bezpieczeństwa danych osobowych są stosowane w danym zakładzie pracy, **decyduje pracodawca**. Decyzja w tym zakresie jest poprzedzana przeprowadzeniem analizy ryzyka. Nie w każdym zakładzie pracy środki te będą więc takie same.

Można wyróżnić następujące środki bezpieczeństwa:

prawne – regulacje prawne wewnątrzzakładowe, obowiązujące u administratora danych osobowych,

organizacyjne – rozwiązania administracyjne,

techniczne:

a) **informatyczne** – środki elektroniczne służące zachowaniu bezpieczeństwa i integralności przetwarzanych danych,

b) **fizyczne.**

Środki prawne

Pracownik musi przestrzegać przepisów wewnątrzzakładowych **przyjętych u danego pracodawcy**.
Środkami prawnymi służącymi bezpieczeństwu przetwarzanych danych mogą być:
polityka prywatności,
instrukcja zarządzania systemem informatycznym,
polityka czystego biurka i czystego ekranu,
ewidencja osób upoważnionych do przetwarzania danych osobowych,
wykaz budynków i pomieszczeń gdzie przetwarza się dane osobowe,
wykaz systemów i programów używanych do przetwarzania danych osobowych.

Środki prawne

Przyjęte wewnątrzzakładowe akty prawne mogą nosić inne nazwy. Niezależnie od użytego nazewnictwa pracownicy mają obowiązek ich przestrzegania, pod warunkiem, że te akty są zgodne z RODO.

Uwaga! Polityka bezpieczeństwa, instrukcja zarządzania systemem informatycznym przyjęte przed 25 maja 2018 r. mogą nadal obowiązywać, jeżeli są zgodne z RODO. Pracownicy są zobowiązani do ich przestrzegania.

Środki organizacyjne

Nie każdy pracownik może mieć dostęp w równym stopniu do wszystkich danych osobowych.

Pracodawca określa, którzy pracownicy mogą odczytywać lub zapisywać konkretne dane osobowe, np.: pracownik sekretariatu może mieć dostęp do danych z książki kontaktowej w postaci imion, nazwisk, firm i adresów - do danych wykonawców czy serwisu).

Środki organizacyjne

Pracownik może przetwarzać dane osobowe tylko w takim zakresie, w jakim został **upoważniony przez pracodawcę**.

Przez przetwarzanie należy rozumieć wszelkie operacje wykonywane na danych osobowych. Chodzi tu więc np. o zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie czy usuwanie.

Przetwarzanie danych bez odpowiedniego upoważnienia lub z przekroczeniem jego zakresu stanowi **naruszenie**, które powinno zostać zgłoszone pracodawcy i IOD (w zależności od ustaleń w danym zakładzie pracy).

Środki organizacyjne

Pracownicy powinni stosować się do wewnątrzzakładowych wytycznych regulujących np. następujące kwestie:

do czego i kto się może logować,

kto ma dostęp do jakich kluczy,

kto przyznaje uprawnienia do poszczególnych systemów (np. finansowo-księgowego, danych o nieobecnościach),

jak postępować w sytuacji naruszenia bezpieczeństwa danych osobowych (np. stwierdzenia wykradzenia danych logowania do systemów IT),

jak często należy zmieniać hasła dostępu do systemów informatycznych.

Środki informatyczne

Bez stosownego upoważnienia pracownicy nie mogą mieć również dostępu do systemów i sieci teleinformatycznych.

Pracownicy powinni przestrzegać również następujących reguł (jeżeli zostały wprowadzone):

a) szyfrowanie nośników pamięci,

b) okres przechowywania elektronicznych nośników informacji zawierających dane osobowe,

c) sporządzanie kopii zapasowych,

d) szyfrowanie wiadomości e-mail,

e) obowiązek zainstalowania oprogramowania antywirusowego na komputerze służbowym lub prywatnym używanym do celów służbowych.

Środki fizyczne

Środkami ochrony fizycznej są środki chroniące pomieszczenia, sprzęt, infrastrukturę czy nawet sam personel administratora danych osobowych.

Ochrona również dotyczy zdarzeń mogących zaistnieć fizycznie i realnie: wandalizm, kradzież, włamanie, klęska żywiołowa, terroryzm, podszycie się pod pracownika administratora danych osobowych.

Środki fizyczne powinny chronić wszelkie rzeczywiście istniejące w przestrzeni obiekty, służące do przetwarzania danych osobowych lub biorące udział w takim przetwarzaniu.

Środki fizyczne

Fizyczne środki bezpieczeństwa danych osobowych możemy podzielić na:

a) **pasywne** – zapobiegające albo opóźniające zagrożenia, np. ogrodzenie, zamek, zasuwa, łańcuch, krata, sejf, kasetka, Kensington Lock,

b) **aktywne** – wykrywające zagrożenia albo im przeciwdziałające, np. monitoring audio/wideo, nadajnik GPS, czujki ruchu, alarm przeciwwłamaniowy, czytnik biometryczny (poniekąd jest to zabezpieczenie także pasywne), system gaśniczy.

Środki fizyczne

Z jakimi środkami fizycznymi mogą spotkać się pracownicy?

przechowywanie danych w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi);

przechowywanie danych w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności ogniowej;

przechowywanie danych w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności na włamanie;

przechowywanie danych w pomieszczeniu, w którym okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej;

przechowywanie danych w pomieszczeniu wyposażonym w system alarmowy przeciwwłamaniowy;

przechowywanie danych w pomieszczeniu objętym systemem kontroli dostępu;

Środki fizyczne

Z jakimi środkami fizycznymi mogą spotkać się pracownicy?

przechowywanie danych w pomieszczeniu kontrolowanym przez system monitoringu z zastosowaniem kamer przemysłowych;

przechowywanie danych w pomieszczeniu, które w czasie nieobecności zatrudnionych tam pracowników jest nadzorowane przez służbę ochrony;

przechowywanie danych w pomieszczeniu, które przez cała dobę jest nadzorowane przez służbę ochrony;

przechowywanie danych w zamkniętej niemetalowej szafie;

przechowywanie danych w zamkniętej metalowej szafie;

przechowywanie danych w zamkniętym sejfie lub kasie pancernej;

Środki fizyczne

Z jakimi środkami fizycznymi mogą spotkać się pracownicy?

przechowywanie kopii zapasowych lub archiwalnych zbioru danych osobowych w zamkniętej niemetalowej szafie;

przechowywanie kopii zapasowych lub archiwalnych zbioru danych osobowych w zamkniętej metalowej szafie;

przechowywanie kopii zapasowych lub archiwalnych zbioru danych osobowych w zamkniętym sejfie lub kasie pancernej;

przetwarzanie danych w kancelarii tajnej, prowadzonej zgodnie z wymogami określonymi w odrębnych przepisach;

przechowywanie danych w pomieszczeniu zabezpieczonym przed skutkami pożaru za pomocą systemu przeciwpożarowego lub wolnostojącej gaśnicy;

niszczenie dokumentów zawierających dane osobowe po ustaniu przydatności w sposób mechaniczny za pomocą niszczarek dokumentów.

Środki fizyczne

Wpływ na bezpieczeństwo przetwarzania danych mają także procesy takie jak usuwanie danych, pseudonimizacja i anonimizacja. Należy odróżniać te pojęcia.

Usuwanie danych

Dane osobowe powinny zostać usunięte bezzwłocznie, jeżeli są zbędne do realizacji celu, dla którego zostały zebrane. Dane powinny być więc usunięte kiedy nie są już potrzebne w kontekście celu dla którego zostały pobrane - kiedy administrator nie ma prawa przetwarzać danych osobowych. Usunięcie danych oznacza definitywne wykasowanie danych z wszelkich nośników danych, w tym także z kopii zapasowych. Obowiązkiem usuwania danych mogą być obarczeni pracownicy.

Środki fizyczne

Anonimizacja

Jeżeli pracodawca nie ma już podstawy prawnej do przetwarzania danych osobowych (np. z powodu przedawnienia) ale z jakichś przyczyn chce zachować umowy, może te umowy zmodyfikować przez usunięcie danych osobowych z treści umów (wyczernienie, wykreślenie, wycięcie w sposób trwale uniemożliwiający odczytanie danych). Obowiązek wykonywania czynności anonimizacyjnych może zostać nałożony na pracowników.

Środki fizyczne

Pseudonimizacja

O ile usunięcie danych osobowych czy to poprzez zniszczenie dokumentu czy anonimizację prowadzi do całkowitej niemożności odtworzenia tożsamości danych osobowych, o tyle spseudonimizowane dane osobowe to takie dane, które przy użyciu dodatkowych informacji można przypisać osobie fizycznej. Po pseudonimizacji mamy więc nadal do czynienia z informacjami o możliwej do zidentyfikowania osobie fizycznej.

Przykłady naruszeń bezpieczeństwa

Pracownik pozostawił dokumenty na biurku mimo, że w danym momencie nie były mu niezbędne do przechowywania zadań. W konsekwencji dostęp do tych danych uzyskała osoba postronna lub inny pracownik, który nie był upoważniony do przetwarzania danych osobowych.

Pracownik pozostawił niewyłączony komputer służbowy na terenie firmy, wskutek czego dostęp do danych osobowych zgromadzonych na tym komputerze zyskała osoba postronna.

Pracownik był upoważniony wyłącznie do przetwarzania danych osobowych klientów. Z uwagi na doświadczenie w sprawach kadrowo-płacowych w dniu 29 października bez wiedzy pracodawcy pełnił „zastępstwo koleżeńskie” za pracownika działu kadr, zyskując tym samym dostęp do danych osobowych innych pracowników – mimo braku stosownego upoważnienia w tym zakresie.

Przykłady naruszeń bezpieczeństwa

Pracownik zaniechał instalacji oprogramowania antywirusowego i firewalla na komputerze prywatnym używanym do celów służbowych, wskutek czego doszło do wykradnięcia danych osobowych klientów.

Pracownik omyłkowo wysłał wiadomość e-mail do osoby, która nie była uprawniona do dostępu do danych osobowych zawartych w tej wiadomości. Dane te nie były zaszyfrowane, mimo, że tak przewidywała obowiązująca u pracodawcy polityka bezpieczeństwa.

Pracownik wysłał tę samą wiadomość e-mail do kilku odbiorców, wpisując w polu: „adresaci” wszystkie adresy e-mail, wskutek czego każdy z odbiorców ma możliwość podglądu adresu skrzynki mailowej innych odbiorców (a adresy te pozwalają na identyfikację osób fizycznych, przez co stanowią dane osobowe).

Pracownik miał wykonać anonimizację danych w niektórych dokumentach. Zdecydował się na użycie korektora, przez co dane nadal można było odczytać.

Przykłady naruszeń bezpieczeństwa

Podczas sprzątania biura pracownik omyłkowo wraz z makulaturą wyrzucił do kosza archiwalne dokumenty zawierające dane osobowe. Nie doszło więc do zniszczenia tych danych i niestety stały się one dostępne dla nieuprawnionych.

Pracownik nie zamknął pomieszczenia z dokumentacją zawierającą dane osobowe na klucz, wskutek czego dostęp do pomieszczenia mogły zyskać osoby postronne.

Pracownik wyniósł bez zgody pracodawcy dokumenty zawierające dane osobowe poza firmę.

Pracownik trzymał na biurku kartkę z loginem i hasłem do wewnątrzzakładowego oprogramowania zawierającego dane osobowe. Kartka była widoczna dla osób postronnych.

Jak postąpić w przypadku naruszenia?

Szczegółowy tryb postępowania w przypadku naruszenia bezpieczeństwa danych osobowych powinny określać przepisy wewnątrzzakładowe (np. procedura postępowania w przypadku naruszeń ochrony danych osobowych).

Jest jednak oczywiste, że każdy pracownik w przypadku stwierdzenia podejrzenia naruszenia przepisów bezpieczeństwa powinien niezwłocznie **zawiadomić** o tym pracodawcę, ewentualnie także inspektora ochrony danych.

Pracownik powinien również pozostawić miejsca zdarzenia w stanie nienaruszonym do czasu przybycia inspektora ochrony danych lub innej osoby uprawnionej.

Należy działać **niezwłocznie**, gdyż administrator danych osobowych ma co do zasady 72 godziny na zgłoszenie naruszenia do Prezesa UODO.

Sankcje

W przypadku naruszeń w zakresie zabezpieczenia danych osobowych pracodawca musi liczyć się z sankcjami w postaci:

administracyjnych kar pieniężnych,

odpowiednich środków nakładanych na mocy RODO przez organ nadzorczy (Prezesa UODO),

upomnienia.

Uwaga! Sankcje nie są wymierzane poszczególnym pracownikom, lecz pracodawcy jako administratorowi danych osobowych.

Sankcje

Pracownik musi jednak liczyć się z odpowiedzialnością za spowodowanie naruszenia ochrony danych osobowych w zakładzie pracy:

Odpowiedzialność materialna

Jeżeli przez naruszenie doszło do wyrządzenia szkody pracodawcy (pracodawca został obciążony karą pieniężną przez Prezesa UODO lub musiał zapłacić odszkodowanie podmiotowi danych), wówczas w trybie roszczenia regresowego pracodawca może zażądać odszkodowania od pracownika. W przypadku wyrządzenia szkody z winy nieumyślnej odszkodowanie nie może przekraczać równowartości **3-miesięcznego wynagrodzenia** pracownika.

Sankcje

Pracownik musi jednak liczyć się z odpowiedzialnością za spowodowanie naruszenia ochrony danych osobowych w zakładzie pracy:

Odpowiedzialność porządkowa

Nawet jeśli pracodawca nie został ukarany za naruszenie ochrony danych osobowych spowodowanych przez pracownika, to i tak pracownik może zostać ukarany karą porządkową **upomnienia lub nagany** za naruszenie porządku pracy. Kara ulega zatarciu (usunięciu z akt osobowych pracownika) po roku nienagannej pracy.

Sankcje

Pracownik musi jednak liczyć się z odpowiedzialnością za spowodowanie naruszenia ochrony danych osobowych w zakładzie pracy:

Zwolnienie dyscyplinarne

W skrajnych przypadkach, jeżeli uchybienie pracownika będzie nosiło znamiona ciężkiego naruszenia podstawowych obowiązków pracowniczych, pracodawca może rozwiązać z pracownikiem umowę o pracę **bez wypowiedzenia**. Ta sankcja może być stosowana w skrajnych przypadkach, np. gdy uchybienie spowodowało wyciek danych osobowych na dużą skalę.

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.	**Pracodawca w 2015 r. wdrożył instrukcję zarządzania systemami informatycznymi w zakładzie pracy. Pracownicy:**
A.	nie powinni jej stosować z uwagi na wejście w życie RODO.
B.	powinni ją stosować.
C.	powinni ją stosować w takim zakresie, w jakim nie jest sprzeczna z RODO i innymi przepisami prawa powszechnie obowiązującego.

TEST WIEDZY

2.	**Pracownik:**
A.	może mieć dostęp do danych osobowych wyłącznie w takim zakresie, w jakim został do tego upoważniony
B.	w szczególnie uzasadnionych przypadkach może mieć dostęp do danych osobowych wykraczających poza zakres upoważnienia.
C.	może bez względu na treść upoważnienia mieć dostęp do wszystkich danych osobowych, jakie przetwarza pracodawca.

TEST WIEDZY

3.	**W jakim terminie pracownik powinien zawiadomić pracodawcę lub inspektora ochrony danych o podejrzeniu naruszenia ochrony danych osobowych w zakładzie pracy**
A.	niezwłocznie
B.	w terminie 72 godzin
C.	w terminie 2 dni roboczych

TEST WIEDZY

4.	**Czy pracownicy mają obowiązek szyfrowania wiadomości e-mail zawierających dane osobowe?**
A.	nie
B.	tak, jeżeli przewidują to przepisy wewnątrzzakładowe np. polityka bezpieczeństwa
C.	tak, w każdym przypadku

TEST WIEDZY

5.	**Nieodwracalne wyczernienie danych osobowych kontrahenta z umowy to:**
A.	niedopuszczalna modyfikacja umowy.
B.	pseudonimizacja danych.
C.	anonimizacja danych.

TEST WIEDZY

6.	**Wyrzucenie dokumentacji zawierającej dane osobowe na śmietnik to:**
A.	naruszenie ochrony danych osobowych (w każdym przypadku).
B.	dopuszczalny sposób usuwania danych osobowych (w każdym przypadku).
C.	dopuszczalny sposób usuwania danych osobowych (jeżeli pozwalają na to przepisy wewnątrzzakładowe).

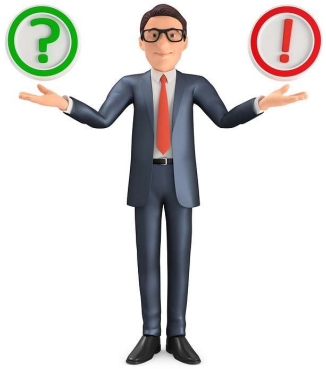
TEST WIEDZY

7.	**Za nieumyślne naruszenie bezpieczeństwa danych osobowych i związany z tym wyciek danych pracownik:**
A.	nie może ponosić odpowiedzialności materialnej.
B.	może ponosić odpowiedzialność materialną w wysokości nie wyższej niż równowartość jego 3-miesięcznej pensji.
C.	może ponosić nieograniczoną odpowiedzialność materialną.

TEST WIEDZY

8.	Pracownik:
A.	może zostać zwolniony dyscyplinarnie za każde doprowadzenie do naruszenia ochrony danych osobowych w zakładzie pracy.
B.	może zostać zwolniony dyscyplinarnie za doprowadzenie do naruszenia ochrony danych osobowych w zakładzie pracy, które jest jednocześnie ciężkim naruszeniem podstawowych obowiązków pracowniczych.
C.	Nie może zostać zwolniony dyscyplinarnie za każde doprowadzenie do naruszenia ochrony danych osobowych w zakładzie pracy.

GRATULUJĘ!!!!



PONIŻEJ PODAJĘ ODPOWIEDZI
ZAPRASZAM DO SAMOOCENY

ODPOWIEDZI

1.	C
2.	A
3.	A
4.	B
5.	C
6.	A
7.	B
8.	B