

SZKOLENIE W SYSTEMIE SAMOKSZTAŁCENIA KIEROWANEGO Z ZAKRESU OCHRONY DANYCH OSOBOWYCH

RODO

MODUŁ 5

Część 1: Zasady ochrony informacji

Część 2: Dokumentacja papierowa zawierająca dane osobowe a praca zdalna

INFORMACJE OD INSPEKTORA OCHRONY DANYCH!!!!

Zaprezentowane materiały mają na celu uczulenie pracowników na kwestie związane z bezpieczeństwem przetwarzania danych osobowych oraz zwiększenie świadomości pracowników w zakresie ochrony danych osobowych.

Do prezentacji dołączony został quiz sprawdzający wiedzę pracowników.

ZAPRASZAM JEDNOCZEŚNIE DO KONTAKTU

iodo@iodo.kutno.pl

Paweł Łuczak: Inspektor Ochrony Danych

Część 1

Zasady ochrony informacji

Zasady ochrony informacji

Dzięki **zasadom ochrony informacji** dowiesz się, jak:

- tworzyć bezpieczne hasła i nimi zarządzać,
- właściwie korzystać z poczty firmowej i zasobów Internetu,
- komunikować się w mediach społecznościowych,
- rozpoznać phishing i jemu zapobiec.

Jaki jest sens RODO?

Do momentu wejścia w życie RODO w Unii Europejskiej nie funkcjonował spójny system ochrony danych osobowych, co – biorąc pod uwagę swobodę przepływu osób, usług i kapitału – jest ważne dla ochrony podstawowych praw i wolności jej obywateli. Dla przeciętnego Kowalskiego ochrona danych osobowych już od dawna nie sprowadza się do walki z natrętnym telemarketingiem. Giganci technologiczni są już bowiem w stanie, poprzez operacje na naszych danych, wpływać na nasze wybory polityczne czy ceny biletów lotniczych kupowanych przez Internet.

Nie jesteś jednak w stanie chronić swojej prywatności, jeśli nie masz wiedzy, kto przetwarza Twoje dane. Z tego powodu RODO wprowadza szereg ważnych postanowień gwarantujących Ci kontrolę nad Twoimi danymi. Takie same prawa mają klienci i kontrahenci Twojej organizacji.

Jaki jest sens RODO?

Oprócz zapewnienia informacji na temat przetwarzania, akt ten zobowiązuje też administratorów danych do stosowania środków technicznych i organizacyjnych, które zapewnią odpowiedni poziom bezpieczeństwa.

RODO wymusza stałe dostosowywanie organizacji do zmieniającej się rzeczywistości – źródłem naruszenia może być każdy człowiek i każdy zasób przetwarzający dane osobowe. Utrata reputacji lub konieczność zapłaty wysokich odszkodowań czy kar finansowych mogłaby odbić się na całym zespole pracowników. Jeśli pracownik naruszy swoje obowiązki musi liczyć się także ze swoją odpowiedzialnością. Dlatego dobro organizacji i jej klientów to także dobro jej pracownika.

Wprowadzenie do bezpieczeństwa informacji

Wydawać by się mogło, że ustawienie monitora lub miejsce przechowywania dokumentów, nie ma dużego wpływu na funkcjonowanie firmy. A jednak służbowe biurko jest wyjątkowym źródłem wiedzy o organizacji. Brak odpowiednich środków bezpieczeństwa, a także lekkomyślne zachowania zarówno zwykłych pracowników, jak i kadry zarządzającej mogą przyczynić się do niezamierzonego udostępnienia cennych informacji.

Najpopularniejszych typów incydentów zwykle można uniknąć, jeśli pracownik nie popełni błędów, takich jak: wysyłka wiadomości pod błędny adres, zgubienie laptopa, pozostawienie niezabezpieczonych dokumentów, praca w domu przy dostępie rodziny i znajomych itd. W tym module dowiesz się, jak w prosty sposób podnieść poziom bezpieczeństwa

Polityka haseł

Najczęstszym źródłem wycieku haseł jest ich właściciel. Dlatego dobrze, abyś stosował się do poniższych zasad:

- nie zapisuj haseł i nie umieszczaj ich w miejscach dostępnych dla innych osób,
- nie stosuj haseł łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących danej osoby, np. imion, numerów telefonu, dat urodzenia itp.,
- nie używaj tych samych haseł w różnych systemach operacyjnych i aplikacjach oraz w życiu służbowym i prywatnym,
- nie zapisuj haseł „na stałe” oraz nie wykorzystuj opcji autozapamiętywania haseł (np. w przeglądarkach internetowych),
- nie twórz haseł w sposób przewidywalny, np. kolejno: HasłoLipiec1!, HasłoSierpień1!, HasłoWrzesień1!
- stosuj „szyfry” polegające np. na: złożeniu hasła z pierwszych liter wyrazów składających się na jakieś zdanie (np. OMGzzh* od Oh My God znowu zapomniałem hasła* czy GJSkś* od Gdzie Jest Słonko kiedy śpi*).

Poczta elektroniczna

Niedozwolone jest wykorzystywanie prywatnej poczty elektronicznej do celów służbowych. Dotyczy to zarówno wysyłania dokumentów i danych na swoje skrzynki prywatne, jak i podawania klientom i kontrahentom swoich adresów prywatnych w celu wymiany korespondencji.

Ponadto podczas korzystania z poczty nie powinno otwierać się załączników takich jak programy wykonywalne (np. z rozszerzeniem .exe), gdyż mogą one zawierać szkodliwe oprogramowanie.

Pamiętaj!

Pracodawca, jeżeli wcześniej poinformuje o tym swoich pracowników i współpracowników (w sposób określony w kodeksie pracy), ma prawo do monitorowania poczty wychodzącej i przychodzącej ze służbowej skrzynki pocztowej oraz przeglądanych stron internetowych.

Zasady przesyłania korespondencji masowej

Częstym naruszeniem bezpieczeństwa danych w masowej korespondencji elektronicznej jest ujawnienie poszczególnych odbiorców wiadomości. Przy masowej wysyłce elektronicznej korespondencji (np. mailingu reklamowym) nie wolno udostępniać innym listy mailingowej, zawierającej dane osobowe pozostałych adresatów takiej wiadomości, ponieważ podlegają one ochronie.

W przypadku wysyłania korespondencji do większej liczby osób poza organizację należy dbać o to, aby osoby, do których skierowana jest tego typu korespondencja, nie miały możliwości zapoznania się z danymi pozostałych adresatów wiadomości – nie tylko ich imionami i nazwiskami, lecz także adresami e-mail.

Używanie adresów służbowych w celach prywatnych

Rejestrowanie się na stronach internetowych do celów prywatnych przy pomocy służbowych adresów e-mail jest niewskazane. Powszechnie udostępniony adres służbowy pozwala przestępcom na zidentyfikowanie pracowników Twojej organizacji i ułatwia im stworzenie bazy danych adresów, które mogą stanowić przedmiot potencjalnego ataku.

Należy pamiętać, że w przypadku adresów służbowych celem ataku nie jest pojedynczy pracownik, ale cała organizacja, która przetwarza dane wielu osób, w związku z czym dane te powinny podlegać szczególnej ochronie.

Używanie adresów służbowych w celach prywatnych

Pamiętaj też, że używając służbowego adresu, reprezentujesz swoją organizację na zewnątrz. Przykładowo, publikując opinie na GoldenLine czy LinkedIn, robisz to jako przedstawiciel organizacji, która Cię zatrudnia – czyń to z rozsądkiem.

Fałszywe wiadomości e-mail (phishing)

Od dłuższego już czasu użytkownicy Internetu otrzymują e-maile łudząco podobne do wysyłanych przez Poczte Polską, firmy kurierskie czy telekomunikacyjne. Spreparowane wiadomości często zawierają załącznik z oprogramowaniem, którego otworzenie powoduje zainfekowanie komputera, a w konsekwencji – wyłudzenie m.in. danych uwierzytelniających do kont bankowych czy zaszyfrowanie zawartości Twojego komputera lub serwera służbowego (bywa, że pojawia się żądanie okupu w zamian za jego odszyfrowanie).

Dlatego zwracaj baczną uwagę na otrzymywane wiadomości:

- przeczytaj uważnie treść e-maila, przyjrzyj się formie – jeśli masz wątpliwości, porównaj ją z innymi e-mailami od tego samego nadawcy,
- zachowaj czujność w przypadku wiadomości w jakikolwiek sposób związanych z kwestiami finansowymi,
- przed kliknięciem w link sprawdź, dokąd prowadzi – jeśli odsyła do formularza, w którym trzeba podać ważne dane, zachowaj ostrożność,
- szczególnie uważaj na e-maile, w których nadawca straszy Cię konsekwencjami lub zbyt wiele obiecuje,
- nie otwieraj załączników, które budzą Twoją wątpliwość,
- zwracaj uwagę na samą treść wiadomości, jej styl oraz jej poprawność językową – błędy mogą spowodować zapalenie się czerwonej lamki, gdyż wiadomości tworzone przez profesjonalne podmioty są co do zasady profesjonalnie sformułowane.

W razie otrzymania podejrzanej wiadomości e-mail pamiętaj o bezzwłocznym powiadomieniu działu IT w swojej organizacji.

Przeglądanie zasobów Internetu

Podczas korzystania z przeglądarek internetowych należy zwracać uwagę na nietypowe rzeczy, które dzieją się podczas pracy. Najbardziej popularne, nieautoryzowane zmiany mogą powodować: wyświetlające się okienka z reklamami, zmianę wyglądu strony, podejrzane linki, reklamy wyświetlające się na stronach internetowych bez możliwości ich zamknięcia.

W sieci pojawił się serwis umożliwiający sprawdzenie, czy dane hasło zostało wykradzione i wyciekło do Internetu. Jeśli w tym momencie zapaliła Ci się czerwona lampka – słusznie. Wpisanie hasła na tej stronie może oznaczać, że jeśli do tej pory Twoje hasło nie wyciekło, to właśnie sam spowodowałeś jego wyciek.

Wypowiedzi na portalach i forach

Niedozwolone jest publikowanie na portalach internetowych danych osobowych stanowiących informację służbową uzyskaną podczas pracy, o ile nie leży to w zakresie obowiązków pracownika.

Niewskazane jest publikowanie wiadomości prywatnych (z zastrzeżeniem ograniczonego wykorzystania dostępu do Internetu do celów prywatnych) na stronach internetowych, na których publicznie widoczny jest adres IP Twojego pracodawcy.

**SERDECZNIE DZIĘKUJĘ ZA UDZIAŁ W
SZKOLENIU.**

ZAPRASZAM DO ROZWIĄZANIA TESTU

W PYTANIU 1,2,3 TYLKO JEDNA ODPOWIEDŹ PRAWIDŁOWA!!!!

W PYTANIU 4 KILKA ODPOWIEDZI PRAWIDŁOWYCH

**BARDZO PROSZĘ W PRZYPADKU JAKICHKOLWIEK PYTAŃ
O KONTAKT:**

iodo@iodo.kutno.pl

Paweł Łuczak: Inspektor Ochrony Danych

TEST WIEDZY

PYTANIE 1

Kiedy pracodawca może monitorować służbową pocztę pracownika?

- a) Po ukończeniu przez pracownika szkolenia z ochrony danych osobowych.
- b) Po wcześniejszym poinformowaniu o tym pracownika.
- c) Zaraz po podpisaniu umowy.
- d) Gdy pracodawca zakupi odpowiednie oprogramowanie.

TEST WIEDZY

PYTANIE 2

Przesyłanie dokumentacji służbowej na prywatny adres poczty elektronicznej jest:

- a) Dopuszczalne za zgodą przełożonego.
- b) Całkowicie zabronione.
- c) Dopuszczalne – przecież muszę dokończyć pracę w domu.
- d) Dopuszczalne – dopóki nikt o tym nie wie.

TEST WIEDZY

PYTANIE 3

Wskaż najtrudniejsze hasło do złamania:

- a) qwerty.
- b) Bożena001.
- c) QwE456PoI654.
- d) Qaz123.

TEST WIEDZY

PYTANIE 4

Wskaż możliwe sygnały ostrzegawcze identyfikujące otrzymaną przez Ciebie wiadomość jako próbę wyludzenia informacji:

- a) Wiadomość zawiera błędy ortograficzne i gramatyczne i nie jest zaadresowana wyłącznie do Ciebie.
- b) Wiadomość zachęca do szybkiego podjęcia działania.
- c) Wiadomość zawiera prośbę o otwarcie załącznika i instalację aktualizacji oprogramowania.
- d) Wiadomość zaadresowana jest do Ciebie.

GRATULUJĘ!!!!



PONIŻEJ PODAJĘ ODPOWIEDZI
ZAPRASZAM DO SAMOOCENY



ODPOWIEDZI

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

CZĘŚĆ 2

Dokumentacja papierowa zawierająca dane osobowe a praca zdalna-

*na podstawie zaleceń Urzędu Ochrony
Danych Osobowych*

Dokumentacja papierowa zawierająca dane osobowe a praca zdalna

Pracodawca w wyjątkowych sytuacjach może zezwolić pracownikom na korzystanie w pracy zdalnej z dokumentacji papierowej zawierającej dane osobowe. Wiąże się to jednak z większym ryzykiem naruszenia bezpieczeństwa danych osobowych oraz związaną z nim koniecznością ich odpowiedniego zabezpieczenia – wyjaśnia UODO.

Dokumentacja papierowa zawierająca dane osobowe a praca zdalna

W obowiązującym obecnie w Polsce stanie epidemii od pracodawców wymaga się zorganizowania pracy w taki sposób, aby ograniczyć osobiste kontakty pomiędzy pracownikami, w szczególności - gdy jest to możliwe - poprzez polecenie im wykonywania pracy zdalnej zgodnie z art. 3 ustawy z 20 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych.

Wobec pojawiających się w związku z tym pytań dotyczących możliwości wykorzystywania przez pracowników świadczących pracę zdalną dokumentacji papierowej zawierającej dane osobowe, UODO przedstawia podstawowe zasady, którymi należy się w takiej sytuacji kierować.

Dokumentacja papierowa zawierająca dane osobowe a praca zdalna

Pracodawcy jako administratorzy danych przetwarzanych przez pracowników podczas pracy zdalnej mają obowiązek zapewnić przestrzeganie zasad przetwarzania danych, w tym zagwarantować ich bezpieczeństwo, biorąc pod uwagę większe ryzyko związane z takimi działaniami. Odnosi się to zarówno do przetwarzania danych przy wykorzystaniu środków komunikacji elektronicznej, jak i danych zawartych w dokumentach papierowych.

Dokumentacja papierowa zawierająca dane osobowe a praca zdalna

Pracownicy podczas pracy zdalnej mogą przetwarzać dane osobowe tylko w celach związanych z wykonywaniem swoich obowiązków służbowych oraz muszą zapewnić ich bezpieczeństwo, przestrzegając wewnętrzne polityki oraz inne procedury przyjęte w tym zakresie przez pracodawcę. Na pracownikach spoczywa również ogólny obowiązek dbałości o dobro zakładu pracy w zakresie ochrony danych osobowych.

Dokumentacja papierowa zawierająca dane osobowe a praca zdalna

Pracownicy nie mogą samowolnie wynosić dokumentacji w postaci papierowej poza określony przez pracodawcę obszar przetwarzania danych!!!!

Dokumentacja papierowa zawierająca dane osobowe a praca zdalna

O ile Kodeks pracy wprost reguluje niektóre kwestie dotyczące ochrony danych osobowych w ramach wykonywania telepracy, to żadne przepisy szczególne nie określają odrębnych wymogów ochrony danych osobowych podczas pracy zdalnej. Dlatego pracodawca, kierując do niej pracownika, musi zapewnić zgodność z ogólnymi przepisami RODO dotyczącymi ochrony i bezpieczeństwa danych osobowych. W tym celu powinien wdrożyć odpowiednie procedury oraz środki organizacyjne i techniczne tak, aby pracownicy mieli wystarczającą świadomość i narzędzia umożliwiające im przestrzeganie przepisów o ochronie danych osobowych.

Dokumentacja papierowa zawierająca dane osobowe a praca zdalna

Pracodawca, decydując się na umożliwienie pracownikom korzystania podczas pracy zdalnej z dokumentacji papierowej, musi podjąć działania mające na celu ograniczenie ryzyka związanego z utratą dostępności, integralności oraz poufności danych.

Pracodawca musi ocenić niezbędność wykorzystywania dokumentacji papierowej podczas pracy zdalnej, biorąc pod uwagę charakter danych, cele dla których są przetwarzane oraz dostępne środki.

Należy przede wszystkim ocenić, czy do wykonania swojej pracy niezbędny jest dostęp do danych osobowych, czy też jest możliwe skorzystanie z dokumentów zanonimizowanych.

Dokumentacja papierowa zawierająca dane osobowe a praca zdalna

Praca na dokumentach papierowych nie będzie uzasadniona, jeżeli pracodawca:

- wdrożył elektroniczny obieg dokumentów, a pracownik ma bezpieczny dostęp do niezbędnych do pracy danych osobowych przy pomocy środków komunikacji elektronicznej;
- ma możliwość szybkiego, sprawnego i bezpiecznego wdrożenia elektronicznego obiegu dokumentacji;
- może udostępnić pracownikowi odpowiednio zabezpieczone (m.in. zaszyfrowane) elektroniczne kopie niezbędnych dokumentów.

Dokumentacja papierowa zawierająca dane osobowe a praca zdalna

UWAGA!!!!

Jeżeli nie jest możliwe zastosowanie żadnego z ww. rozwiązań, warto zastanowić się nad pracą na kopiach niezbędnych dokumentów. Minimalizuje to ryzyko naruszenia integralności danych oraz utraty ich dostępności. Należy jednak pamiętać, że pracownik musi chronić dane zawarte w takich dokumentach, tak samo jak w dokumentacji oryginalnej.

Dokumentacja papierowa zawierająca dane osobowe a praca zdalna

Pracodawca, decydując o możliwości wykorzystywania przez pracowników dokumentacji papierowej podczas pracy zdalnej musi:

- zapewnić ewidencjonowanie wydanych pracownikom dokumentów zawierających dane osobowe;
- zapewnić, że udostępnione dokumenty będą przechowywane przez pracownika przez okres niezbędny do wykonania określonego zadania podczas pracy zdalnej (ograniczenie przechowywania);
- ograniczyć liczbę dokumentów wnoszonych z siedziby administratora do tego, co niezbędne w stosunku do celu przetwarzania danych osobowych przez pracownika w ramach pracy zdalnej;
- zobowiązać pracownika do odpowiedniego zabezpieczenia danych osobowych podczas wnoszenia dokumentacji (np. wnoszenie dokumentów w zabezpieczonej aktówce, przenoszenie dokumentów np. w taki sposób, aby były niewidoczne dla osób trzecich);

Dokumentacja papierowa zawierająca dane osobowe a praca zdalna

- zobowiązać pracownika do odpowiedniego zabezpieczenia danych w miejscu wykonywania pracy zdalnej (np. przechowywanie dokumentów w zamykanych na klucz szufladach biurka lub szafach, przestrzeganie zasady czystego biurka, zabezpieczenie dokumentów przed wglądem nieuprawnionych osób trzecich, m.in. członków rodziny);
- zapewnić, że pracownik będzie wykorzystywał pozyskane dane osobowe wyłącznie w tym celu, w jakim byłyby wykorzystywane w siedzibie zakładu pracy;
- określić procedurę związaną z niszczeniem dokumentów (zakaz wyrzucania dokumentów do kosza w domu. Jeżeli pracownik nie posiada w domu niszcarki, powinien dokumenty przechowywać w bezpieczny sposób, a po zakończeniu pracy zdalnej zniszczyć je w biurze);
- zapewnić, że pracownik będzie zgłaszał pracodawcy każdy incydent bezpieczeństwa zgodnie z procedurą postępowania w sprawie naruszeń ochrony danych, tak aby administrator mógł się wywiązać z obowiązku nałożonego na mocy art. 33 ust. 1 RODO.

SERDECZNIE DZIĘKUJĘ ZA UDZIAŁ W SZKOLENIU.
BARDZO PROSZĘ W PRZYPADKU JAKICHKOLWIEK
PYTAŃ O KONTAKT:

iodo@iodo.kutno.pl

Paweł Łuczak: Inspektor Ochrony Danych