Zalecenia Inspektora Ochrony Danych Osobowych w kwestii bezpiecznej pracy zdalnej zgodnej z RODO.

Szanowni Państwo,

W związku z coraz liczniejszymi przypadkami zachorowań na wirusa SARS-CoV-2, który wywołuje chorobę COVID-19, Administrator podjął decyzję o umożliwieniu pracownikom pracy zdalnej, zgodnie z Art. 3 projektu Ustawy dotyczącej wirusa, który mówi iż *w celu przeciwdziałania COVID-19 pracodawca może polecić pracownikowi wykonywania obowiązków wobec pracodawcy, w określonym czasie w domu - praca zdalna*.

Należy pamiętać o zminimalizowaniu kontaktu z dużymi grupami ludzi (duże skupiska ludzi to środowisko sprzyjające rozprzestrzenianiu się koronawirusa) oraz omijaniu miejsc publicznych. Zaleca się pozostanie w domach.

Biorąc pod uwagę powyższy fakt, należy pamiętać, iż w przypadku pracy zdalnej wszelkie dane, które przetwarzane są przez pracownika poza miejscem pracy muszą zostać odpowiednio zabezpieczone. Za zabezpieczenie danych bezpośrednio odpowiada pracownik. Zabezpieczeniu podlegają zarówno dane zgormadzone na nośnikach elektronicznych, jak i papierowych.

Pamiętajmy również, iż nośniki danych typu pendrive mogą być łatwo zgubione, ponieważ ich gabaryty są zwykle małe. Podczas pracy zdalnej należy używać szyfrowanych dysków zewnętrznych (najlepiej typu flash), aby uniknąć przypadkowej utraty danych poprzez ich zagubienie lub mechaniczne uszkodzenie. Ponadto pendrive-y nieznanego pochodzenia często są wykorzystywane przez hakerów do zainstalowania złośliwego oprogramowania na komputerze ofiary ataku. Warto pamiętać o tym podczas używania urządzeń USB nieznajomego pochodzenia.

Poniżej kilka „zagrożeń", o których powinniśmy pamiętać:

Poniżej dołączam zasady bezpieczeństwa informacji, którymi należy się kierować podczas pracy zdalnej:

1) Pracownik jest zobowiązany zachować poufność przetwarzanych danych oraz sposobów ich zabezpieczenia.
2) Dane można wykorzystywać wyłącznie do celów, dla których zostały udostępnione.
3) Dokumenty zawierające informacje podlegające ochronie powinny być przechowywane na biurku i innych miejscach do tego przeznaczonych, w taki sposób, aby osoba nieuprawniona nie miała do nich dostępu.
4) Nośników informacji (w formie papierowej i elektronicznej) z danymi podlegającymi ochronie nie można pozostawiać w miejscach ogólnodostępnych i niezabezpieczonych oraz nie należy udostępniać osobom nieupoważnionym.

5) Dokumenty zawierające informacje podlegające ochronie, przed wyrzuceniem do kosza należy zanonimizować, w taki sposób, aby nie można było odtworzyć ich treści i zidentyfikować osoby, której dane dotyczą, lub zniszczyć za pomocą niszczarki.
6) Monitor należy usytuować w taki sposób, aby osoby nieupoważnione wchodzące do pomieszczenia nie miały wglądu do danych na nim wyświetlanych.
7) Przed zalogowaniem się do systemu stacji roboczej należy upewnić się, że w pobliżu nie ma osób trzecich lub urządzeń nagrywających mogących zarejestrować hasła dostępowe do systemów, z których zamierzamy skorzystać. Jeśli występuje takie zagrożenie należy zastosować szczególne środki ostrożności uniemożliwiające zarejestrowanie wpisywanego hasła.
8) Używanych identyfikatorów i haseł nie należy udostępniać innym osobom, a w przypadku podejrzenia, że osoba postronna weszła w ich posiadanie, należy dokonać ich zmiany zgodnie z obowiązującymi procedurami.
9) Logowanie do systemu pocztowego przy pomocy internetowej przeglądarki powinno być przeprowadzone na osobistym komputerze, laptopie posiadającym zabezpieczenie antywirusowe.
10) Hasła dostępowe do konta pocztowego, systemów informatycznych należy chronić przed dostępem osób trzecich. Nie zaleca się zapamiętywania ich w przeglądarkach internetowych.
11) Po zakończeniu pracy należy wylogować się ze wszystkich systemów, z których korzystaliśmy.
12) Przy opuszczaniu miejsca pracy należy zachować „zasadę czystego biurka" - nośniki informacji umieścić w szafach, szufladach i innych do tego przeznaczonych miejscach oraz upewnić się, że pokój jest zamknięty, gdy jesteśmy jedyną osobą opuszczającą pomieszczenie.
13) Nośniki elektroniczne zawierające informacje podlegające ochronie, poza miejscem pracy należy zabezpieczyć za pomocą środków kryptograficznych.
14) Poza miejscem pracy należy rozmów dotyczących informacji służbowych podlegających ochronie.
15) Dokumenty zawierające dane osobowe w formie papierowej, należy przechowywać w obszarze przetwarzania danych w pomieszczeniach zabezpieczonych drzwiami zamykanymi na klucz w szafach zamykanych na klucz.

W razie jakichkolwiek pytań lub wątpliwości, służę pomocą.

Janusz Wyspiański

Z poważaniem.

Janusz Wyspiański