Praca zdalna (*home office*) w kontekście RODO

MATERIAŁ SZKOLENIOWY DLA PRACOWNIKÓW W ZWIĄZKU Z WYKONYWANIEM PRACY ZDALNEJ

w związku z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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 (ogólne rozporządzenie o ochronie danych)

opracowanie własne

O pracy zdalnej

- Pracodawca może zlecić pracownikowi przejście na pracę zdalną, **w związku z przeciwdziałaniem COVID-19 na podstawie art. 3 tzw. specustawy dotyczącej koronawirusa**
- Praca zdalna to coś innego niż telepraca i może odbywać się nawet bez komputera czy dostępu do firmowych systemów (pracą zdalną może być np. analiza dokumentów czy odręczne napisanie opinii)
- Pracę zdalną zdalna wykonywana jest poza miejscem jej stałego wykonywania – najczęściej w domu
- Dokumentowanie pracy zdalnej to kwestia uzgodnień pomiędzy pracodawcą a pracownikiem
- Polecenie pracy zdalnej nie musi być wydane na piśmie
- Praca zdalna nie zmienia wynagrodzenia pracownika

Twoje obowiązki

- Przestrzegaj zakazu prowadzenia rozmów w miejscach, które nie gwarantują zachowania poufności
- Nie udostępniaj dokumentów papierowych oraz urządzenia, na którym pracujesz, domownikom, współlokatorom lub innym osobom postronnym
- Korzystaj tylko z domowej sieci bezprzewodowej lub z sieci przez Ciebie udostępnionych (hotspot z Twojego urządzenia mobilnego)
- Stosuj zabezpieczenia wdrożone przez Twojego pracodawcę jak: używanie filtrów prywatyzujących, aktualizowanie oprogramowania, blokowanie komputera, zabezpieczenia dokumentów papierowych, łącznie się z siecią firmy przy wykorzystaniu szyfrowanego połączenia VPN z zasobami firmowymi
- Nie drukuj dokumentów firmowych w ogólnodostępnych punktach ksero
- Nie wrzucaj dokumentów firmowych do śmietnika – przechowuj je do momentu bezpiecznego zniszczenia
- Nie dziel się informacjami służbowymi z na portalach społecznościowych
- Pilnuj urządzenia oraz dokumentów papierowych, na których pracujesz, ponieważ mogą ulec zniszczeniu lub zostaną zgubione, a ważne informacje związane z Twoją pracą mogą zostać ujawnione nieuprawnionym osobom

Poczta elektroniczna

- Niedozwolone jest wykorzystywanie prywatnej poczty elektronicznej do celów służbowych
- Niedozwolone jest wysyłanie dokumentów oraz danych na prywatne skrzynki, jak i podawania klientom czy kontrahentom prywatnych adresów w celu wymiany korespondencji
- Niedozwolone jest otwieranie załączników z programami wykonywalnymi (np. z rozszerzeniem .exe), gdyż mogą zawierać szkodliwe oprogramowanie

Pracując zdalnie uważaj na PHISHING

- Fałszywe (specjalnie spreparowane) wiadomości, które są łudząco podobne do wysyłanych przez Pocztę Polską, firmy kurierskie czy telekomunikacyjne

często takie e-maile zawierają załącznik z oprogramowaniem lub link do niego, a otworzenie takiego załącznika powoduje zainfekowanie komputera, a w konsekwencji wyłudzenie danych uwierzytelniających do kont bankowych czy zaszyfrowanie zawartości komputera lub serwera służbowego (bywa, że pojawia się żądanie zapłaty okupu w zamian za odszyfrowanie)

Aby nie paść ofiarą PHISHINGU

- Przeczytaj uważnie treść e-maila, przyjrzyj się jego formie – jeśli masz wątpliwości, porównaj wiadomość z innymi e-mailami od tego samego nadawcy
- Zachowaj czujność w przypadku otrzymania wiadomości w jakikolwiek sposób związanej 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
- Patrz na treść wiadomości, jej styl oraz poprawność językową – błędy mogą być sygnałem ostrzegawczym, gdyż teksty tworzone przez profesjonalne podmioty są co do zasady prawidłowo sformułowane

Przeglądanie zasobów sieci Internet

- Podczas korzystania z przeglądarek internetowych zwróć uwagę na nietypowe rzeczy, które dzieją się w trakcie pracy (np. reklamy bez możliwości ich zamknięcia, zmiana widoku strony)
- Uważaj na portale, które służą do wyłudzania danych osobowych oraz haseł
- Nie podawaj służbowych ani prywatnych informacji na stronach, których pochodzenia nie jesteś pewny/a
- O braku wiarygodności portalu może świadczyć np. brak szyfrowania SSL (kłódka z lewej strony adresu WWW) lub pojawianie się okienek reklamowych, których nie można zamknąć

Raportuj naruszenie ochrony danych gdy

- Nastąpi kradzież albo zagubienie nieszyfrowanego laptopa lub pamięci zewnętrznej (dysku USB), zawierających dane osobowe
- Wyślesz e-maila do wielu odbiorców w kopii otwartej (kopia DW)
- Nastąpi nieuprawnione użycie systemu informatycznego (np. włamanie do systemu informatycznego),
- Dojdzie do wykrycia informatycznego urządzenia lub programu służącego do przechwycenia haseł czy danych
- Porzucisz lub zawieruszysz wydruki dokumentów (szczególnie w dużych ilościach)
- Nieprawidłowo zniszczysz dokumenty papierowe lub elektroniczne na komputerze lub nośników danych (pendrive, płyty CD/DVD)

Jeśli dane osobowe znajdą się w niebezpieczeństwie reaguj

- Skontaktuj się z Inspektorem Ochrony Danych w Twoim miejscu pracy
- Niezwłocznie powiadom swojego pracodawcę - to on jest Administratorem Danych Osobowych
- Jeżeli naruszenie niesie za sobą wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Twój pracodawca:

- zgłosi zdarzenie do Urzędu Ochrony Danych Osobowych
- zostaną powiadomione o zdarzeniu właściwe osoby/osoba