Zasady pracy zdalnej a RODO - poradnik

Przygotuj swoją firmę, czy organizację do stosowania nowych zasad pracy zdalnej. Opisane w tym artykule zasady bezpiecznej pracy zdalnej będą dla Ciebie pomocne przy opracowaniu:

- Regulaminu pracy zdalnej
- Zasad pracy zdalnej
- Szkolenia dla pracowników z zakresu pracy zdalnej

Czym jest praca zdalna i dlaczego czytam ten artykuł?

Praca zdalna polega na możliwości świadczenia pracy poza zakładem pracy, najczęściej z prywatnego mieszkania lub domu. Od 7 kwietnia 2023 roku, praca zdalna została wskazana jako jedna z możliwych form świadczenia pracy w kodeksie pracy.

Opisane w tym artykule przykładowe zasady ochrony danych dotyczą zarówno pracowników, jak i współpracowników - niezależnie od formy zatrudnienia.

Kto może korzystać z pracy zdalnej?

Z możliwości pracy w formie pracy zdalnej mogą korzystać pracownicy na wszystkich stanowiskach. Pod jednym, bardzo ważnym warunkiem - że jest możliwe jej wykonywanie w formie zdalnej ze względu na organizację pracy lub rodzaj pracy.

Kiedy pracodawca musi zapewnić pracownikowi możliwość pracy zdalnej?

Pracodawca nie może odmówić pracy zdalnej w przypadku:

- pracownicy w ciąży,
- pracownikowi wychowującemu dziecko do ukończenia przez nie 4 roku życia,
- pracownikowi sprawującemu opiekę nad innym członkiem najbliższej rodziny lub inną osobą pozostającą we wspólnym gospodarstwie domowym, posiadającymi orzeczenie o niepełnosprawności albo orzeczenie o znacznym stopniu niepełnosprawności,
- pracownikowi-rodzicowi dziecka posiadającego zaświadczenie, o ciąży powikłanej oraz w sytuacji niepowodzeń położniczych,

- pracownikowi-rodzicowi dziecka legitymującego się orzeczeniem o niepełnosprawności albo orzeczeniem o umiarkowanym lub znacznym stopniu niepełnosprawności określonym w przepisach o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych (nawet po ukończeniu przez nie 18 roku życia),
- pracownikowi-rodzicowi dziecka posiadającego odpowiednio opinię o potrzebie wczesnego wspomagania rozwoju dziecka, orzeczenie o potrzebie kształcenia specjalnego lub orzeczenie o potrzebie zajęć rewalidacyjno-wychowawczych (nawet po ukończeniu przez nie 18 roku życia).

Dlaczego RODO jest istotne w czasie pracy zdalnej?

Praca zdalna jest sytuacją win-win: i dla pracownika i pracodawcy. Pod jednym, bardzo ważnym warunkiem - że jest bezpieczna.

Urządzenia i systemy informatyczne, z których korzystają pracownicy w codziennej pracy służą do przetwarzania danych osobowych tysięcy osób. Często są to wrażliwe informacje takie jak PESEL, czy wysokość wynagrodzenia.

Bezpieczeństwo to gra zespołowa. Obowiązkiem działu IT jest zabezpieczenie urządzeń i systemów przed wyciekiem, czy utratą danych. A obowiązkiem pracownika (szczególnie „zdalnego") rozważne i zgodne z procedurami korzystanie z tych narzędzi.

Jeśli któregokolwiek elementu w tej współpracy zabraknie - służbowe dane będą narażone na ogromne niebezpieczeństwo.

Czym jest bezpieczne środowisko pracy zdalnej?

Jeśli pracujesz w biurze, w ramach zespołu, wszyscy pracujecie na podobnych kategoriach danych osobowych.

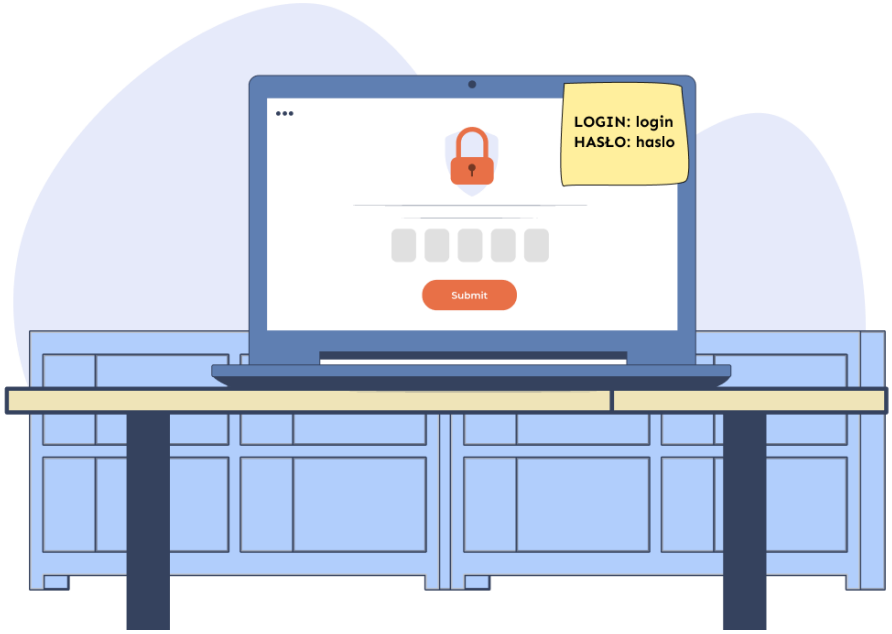
Współdomownicy „zdalnego” pracownika czy jego goście, to zupełnie inna kategoria osób.

To osoby nieupoważnione, które nie mogą mieć dostępu do służbowych danych które przetwarza pracownik zdalny.

W czasie pracy zdalnej pracownik ma obowiązek zadbać, żeby był jedyną osobą, która słyszy i widzi informacje, które są własnością pracodawcy.

W przypadku przetwarzania danych wrażliwych, w tym danych osobowych, monitory powinny być dodatkowo wyposażone w filtry prywatyzujące i ustawione w sposób uniemożliwiający podgląd osobom trzecim.

Domownicy „zdalnego” pracownika nie mogą korzystać z jego sprzętu służbowego. Nie mogą też znać jego loginów i haseł. Pracownik odpowiada również za to, żeby jego domownicy nie weszli w posiadanie jego loginu i hasła w sposób pośredni.



W niektórych miejscach pracy dozwolona jest praca na własnym, prywatnym sprzęcie - smartfonie lub laptopie. W takim przypadku, pracownik bezwzględnie musi zabezpieczyć sprzęt zgodnie z zaleceniami działu IT. Musi też działać zgodnie z obowiązującą w organizacji procedurą BYOD, czyli bring your own device.

Jak bezpiecznie połączyć się z siecią internet?

Pracownik „zdalny" do łączenia się z interntem powinien korzystać z sieci domowej lub hotspotu z własnego telefonu. Hasło do sieci WiFi powinno być zabezpieczone silnym hasłem. Co to znaczy silne hasło?

Zgodnie z najnowszymi wytycznymi CERT, czyli polskiej instytucji zajmującej się cyberbezpieczeństwem, silne hasło to hasło, które:

- jest unikalne, czyli nie jest stosowane nigdzie indziej
- ma minimum 12 znaków
- nie zawiera żadnych przewidywalnych członów jak: Twoje imię, imię Twoich dzieci, współmałżonka, zwierzątka, nazwa ulubionego klubu sportowego
- nie znajduje się na liście najpopularniejszych haseł: np. 123456, qwerty, password

Wskazówka od CERT Polska dla działów IT:

CERT Polska publikuje polską wersję słownika haseł będącą wynikiem analizy danych upublicznionych w wyciekach. Zawiera on zestaw około miliona najpopularniejszych haseł, posortowanych malejąco od haseł najbardziej popularnych. Może on posłużyć administratorom systemów przy wdrożeniu polityki haseł zgodnej z zaleceniami.

Czy można pracować zdalnie tylko z terytorium Polski?

Pracę zdalną pracownik powinien realizować wyłącznie w miejscu uzgodnionym wcześniej z pracodawcą. Jeśli na przykład na wskazał pracodawcy swój adres zamieszkania, a planuje pracować zdalnie z innej lokalizacji, koniecznie powinien uzgodnić to z przełożonymi.

Dotyczy to **szczególnie** przypadków, jeśli pracownik planujee pracować zdalnie spoza terytorium Polski.

Praca zdalna co do zasady powinna być zakazana z terytorium państw nienależących do Europejskiego Obszaru Gospodarczego. Czyli NIE należy do Unii Europejskiej, ani nie jest Islandią, Norwegią i Liechtensteinem.

Jak pracować z dokumentacją papierową?

Pracodawca powinien stworzyć takie środowisko pracy, żeby „zdalny" pracownik nie musiał korzystać z dokumentów papierowych. W dzisiejszych czasach wykonywanie większości prac biurowych jest możliwych w 100% na dokumentach elektronicznych.

Jeśli jednak pracownik musi korzystać z papierowych dokumentów, ma obowiązek ich zwrotu do biura. Albo ich zniszczenia, kiedy przestaną być przydatne. Pracodawca powinien umożliwić pracownikowi dostęp do niszczarek do dokumentów przynajmniej na obszarze swojego biura.

Domownicy „zdalnego" pracownika nie powinni mieć dostępu do dokumentów papierowych. „Zdalny" pracownik powinien posiadać szafkę lub szufladę zamykaną na klucz.

Co z backupem podczas pracy zdalnej?

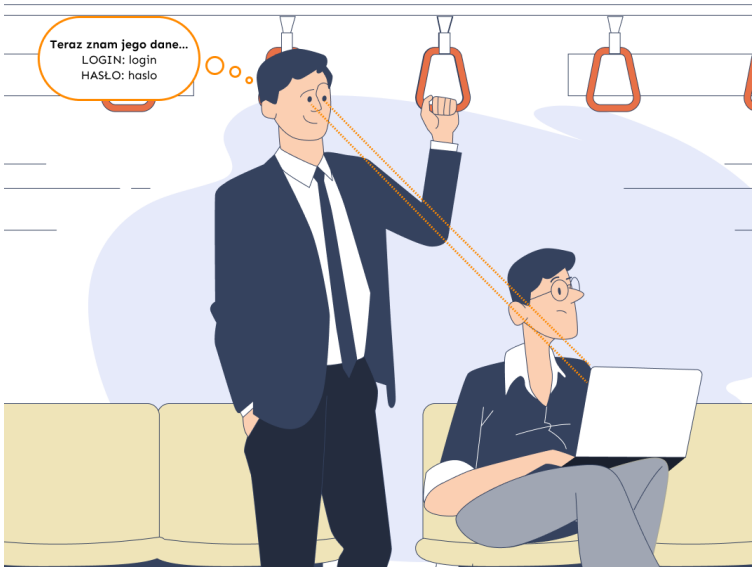
W dzisiejszych czasach bardzo powszechne jest korzystanie z chmurowych rozwiązań i systemów dostępnych z poziomu przeglądarki internetowej. Dlatego też bardzo rzadko dochodzi do sytuacji, żeby na sprzęcie lokalnym pracownika pracującego zdalnie znalazła się JEDYNA kopia danych osobowych.

Dlatego też, dane wymagające backupowania pracownik powinien przechowywać na dyskach sieciowych. Pracownik „zdalny" powinien mieć świadomość, że odpowiada za zabezpieczenie i utratę danych przechowywanych na dyskach lokalnych (na przykład C: i D:).

Jakie są największe zagrożenia w toku pracy zdalnej?

Pracując zdalnie wszyscy musimy liczyć się z większym ryzykiem wystąpienia naruszeń ochrony danych osobowych. Poniżej znajduje się lista przykładowych zagrożeń w toku pracy zdalnej:

- „Zdalny" pracownik transportuje sprzęt komputerowy znacznie częściej niż w czasie pracy z biura. Rosną więc ryzyka jego zgubienia albo kradzieży. Pracownik „zdalny" nie może zostawiać laptopa w miejscach publicznych, czy w aucie.
- Pracując zdalnie w środkach transportu czy innych miejscach publicznych „zdalny" pracownik musi zwrócić uwagę na to, żeby osoby trzecie nie miały możliwości podsłuchania lub podejrzenia jego ekranu.



- Pracując w biurze, pracownik korzysta na ogół z jednej, dobrze zabezpieczonej sieci WIFI. Przy pracy zdalnej jego urządzenie może logować się do wielu różnych sieci. Zwłaszcza, jeśli

podróżuj. Pracownik „zdalny” powinien być świadomy, żeby zwracać uwagę na to, żeby były to sieci zaufane i bezpieczne z szyfrowanym połączeniem wymagającym podania hasła.

- Znasz tego mężczyznę?

To najbardziej znany haker i socjotechnik, Kevin Mitnick. Chociaż akurat TEN Pan już swoje odsiedział i nie przestał być groźny, to nadal pracodawca musi pamiętać, że, pracownik „zdalny” jest jest bardziej narażony na ataki socjotechniczne. Mogą być do nich wykorzystani nawet jego domownicy czy znajomi (również nieświadomie).

Może ktoś podający się za przełożonego w bardzo realistyczny sposób poprosi domownika „zdalnego" pracownika o pilne udostępnienie jego loginu i hasła. Jeśli domownicy „zdalnego" pracownika mają dostęp do takich informacji, ryzyka rosną.

Czy w czasie pracy zdalnej można instalować nowe aplikacje i programy?

Obowiązują podobne zasady jak podczas pracy w biurze. Nowe aplikacje, programy i rozszerzenia do przeglądarki mogą być instalowane wyłącznie, jeśli są konieczne do wykonania pracy oraz po uznaniu ich za bezpieczne przez Dział IT.
Co do zasady, służbowy sprzęt i systemy informatyczne (również urządzenia mobilne) powinny być wykorzystywane do celów służbowych. Korzystanie ze służbowego sprzętu do innych celów niż służbowy powinno być wyjątkiem od reguły i odbywać się wyłącznie na zasadach określonych przez dział IT.

Jak bezpiecznie korzystać z poczty e-mail?

Korzystanie z poczty elektronicznej generuje trzy główne rodzaje ryzyk.

1. **UDW / BCC**

Pracownik „zdalny" może przypadkowo udostępnić dane osobowe.

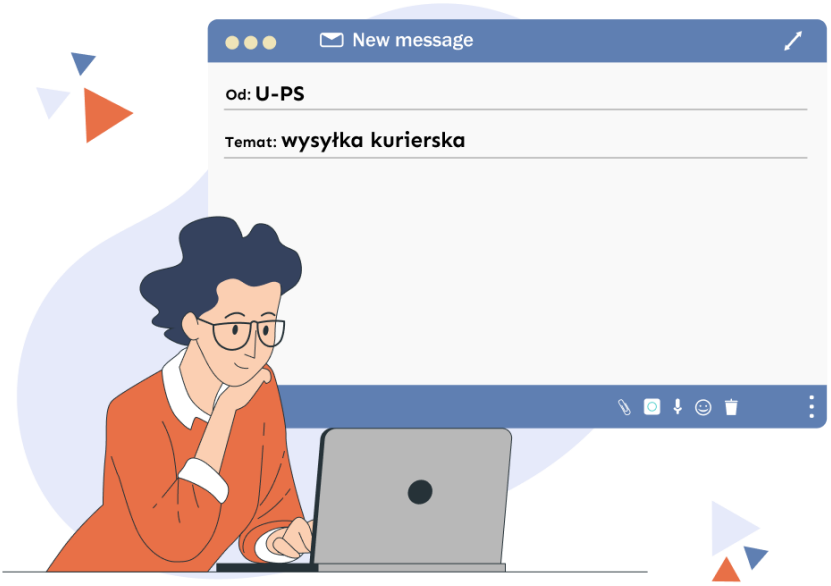
Jak pewnie pamiętasz z poprzednich naszych artykułów - już sam tylko adres e-mail może być danymi osobowymi.

Wysyłając korespondencję do wielu adresatów, bez zastosowania opcji UDW, możesz spowodować naruszenie ochrony danych osobowych.

2. Phsishing

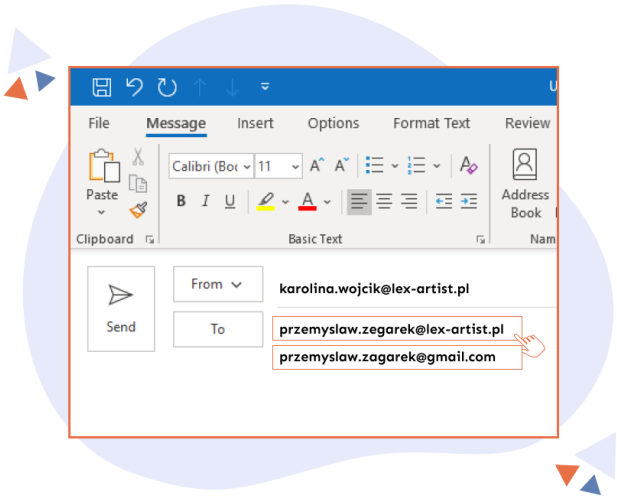
Pracownik „zdalny” powinien zachować szczególną ostrożność, jeśli otrzymał od niezaufanego adresata podejrzane załączniki i linki. Możesz „uodpornić” swoich pracowników na tego typu phishingowe praktyki i pokazać mu nasze bezpłatne szkolenie: Cyberbezpieczny pracownik (security awareness).

Pracownik powinien każdorazowo zgłaszać takie podejrzane wiadomości e-mail do Działu IT.



3. Szyfrowanie

Załączane przez pracowników pliki zawierające dane osobowe i inne poufne informacje mogą trafić przez pomyłkę do adresata o podobnym imieniu i nazwisku.



Żeby uniknąć takiego ryzyka pracownik powinien szyfrować pliki zawierające poufne informacje. Hasło powinien przesłać osobnym kanałem komunikacji (np. SMSem).

Jak zachować się w przypadku naruszenia ochrony danych osobowych?

Pracując zdalnie wszyscy musimy liczyć się z większym ryzykiem wystąpienia naruszeń ochrony danych osobowych. Pracownik „zdalny" powinien być świadom, że w takich sytuacjach od szybkości jego reakcji BARDZO dużo zależy. W wielu przypadkach organizacje będą miał tylko 72 godziny na zgłoszenie naruszenia ochrony danych do UODO.

Dlatego bardzo ważne jest, żeby w takich przypadkach pracownik „zdalny" postępował zgodnie z procedurami postępowania związanymi z naruszeniem ochrony danych osobowych. I żeby niezwłocznie poinformował odpowiednie osoby odpowiedzialne za RODO w organizacji.

Czy pracodawca może skontrolować pracownika w prywatnym mieszkaniu?

Tak, według przepisów zmienionego kodeksu pracy, pracodawca może skontrolować "zdalne" stanowisko pracy. Celem kontroli będzie weryfikacja, czy jest ono faktycznie bezpieczne oraz czy zasady i regulaminy pracy zdalnej są przestrzegane przez pracownika.

Pracodawca może też skontrolować to, jak pracownik „zdalny" wykorzystuje swój czas pracy i czy wykorzystuje otrzymane służbowe urządzenia i materiały zgodnie z ich przeznaczeniem.

Pracodawca, za pośrednictwem bezpośredniego przełożonego może przeprowadzić kontrolę w miejscu wskazanym przez pracownika jako miejsce świadczenia pracy. Na przykład w jego miejscu zamieszkania. Pracodawca zobowiązuje się, że wykonywanie czynności kontrolnych nie będzie naruszało prywatności ani pracownika „zdalnego", ani jego rodziny.

Kontrolę pracodawca powinien zapowiedzieć z odpowiednim wyprzedzeniem.

Jakie konsekwencje grożą pracownikowi za brak stosowania się do zasad pracy zdalnej?

Tak jak zaznaczaliśmy na początku, praca zdalna może być korzystna dla obu stron: i dla pracodawcy i dla pracownika.

Ale pod jednym bardzo ważnym warunkiem - jeśli będzie bezpieczna.

Konsekwencje niestosowania się do przedstawionych zasad, będą zależeć od stopnia ich naruszenia przez pracownika. Może być to wyłączenie możliwości pracy zdalnej, upomnienie, nagana albo rozwiązanie umowy.

Podsumowanie

Praca zdalna może być komfortowym rozwiązaniem. Pracownik „zdalny" musi jednak pamiętać, że jest też druga strona tego medalu. Praca zdalna to też dodatkowe ryzyka i dodatkowe obowiązki, jakie wiążą się z koniecznością zabezpieczenia służbowych danych.

A niestety, wraz z rozwojem technologii umożliwiających i usprawniających pracę zdalną, rośnie też kreatywność cyber-przestępców.

Dlatego, żeby bezpiecznie przetwarzać dane służbowe w czasie pracy zdalnej, pracownik zdalny musi znać i stosować się do wszystkich obowiązujących w miejscu pracy zasad bezpieczeństwa informacji.

Pracownik „zdalny" musi też oczywiście zapoznać się ze szczegółowymi regulaminami, procedurami instrukcjami pracy zdalnej obowiązującymi w organizacji.

Autor artykułu:

Łukasz Zegarek, Ekspert ds. ochrony danych osobowych

Źródła:

- Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. 1974 Nr 24 poz. 141) https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20230000240
- Rozporządzenie 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) (Dz. Urz. UE. L Nr 119, str. 1) https://eur-lex.europa.eu/eli/reg/2016/679/oj/pol