Urząd Ochrony Danych Osobowych

Artykuł: 17.03.2020

https://uodo.gov.pl/pl/138/1459

Ochrona danych osobowych podczas pracy zdalnej

Jak postępować podczas pracy zdalnej, aby nie naruszyć przepisów o ochronie danych? Jakie zabezpieczenia rekomendować pracownikom?

Środki kontroli i zapobiegania rozprzestrzenianiu się COVID-19 będą wymagały większej liczby osób pracujących zdalnie niż zwykle. Poniżej znajduje się kilka porad dotyczących bezpieczeństwa danych osobowych podczas pracy poza biurem.

Załączone pliki

Ochrona danych osobowych podczas pracy zdalnej

OCHRONA DANYCH OSOBOWYCH PODCZAS PRACY ZDALNEJ

URZĄD OCHRONY DANYCH OSOBOWYCH

Środki kontroli i zapobiegania rozprzestrzenianiu się COVID-19 będą wymagały większej liczby osób pracujących zdalnie niż zwykle. Poniżej znajduje się kilka porad dotyczących bezpieczeństwa danych osobowych podczas pracy poza biurem.

URZĄDZENIA

- Urządzenia i oprogramowanie przekazane przez pracodawcę do pracy zdalnej służą do wykonywania obowiązków służbowych. Dlatego też należy postępować zgodnie z przyjętą w organizacji procedurą bezpieczeństwa.

- Nie instaluj dodatkowych aplikacji i oprogramowania niezgodnych z procedurą bezpieczeństwa organizacji

- Upewnij się, że wszystkie urządzenia z jakich korzystasz mają niezbędne aktualizacje systemu operacyjnego (IOS lub Android), oprogramowania oraz systemu antywirusowego.

- Zanim przystąpisz do pracy, wydziel sobie odpowiednią przestrzeń, tak aby ewentualne osoby postronne, nie miały dostępu do dokumentów, nad którymi pracujesz. Odchodząc od stanowiska pracy każdorazowo blokuj urządzenie, na którym pracujesz.

- Zabezpieczaj swój komputer poprzez używanie silnych haseł dostępu, wielopoziomowe uwierzytelnianie. Pozwoli to na ograniczenia dostępu do urządzenia, a jednocześnie na ograniczenia ryzyka utraty danych w przypadku kradzieży lub zgubienia urządzenia

- Podejmij szczególne środki, aby urządzenia z których korzystasz podczas pracy, szczególnie te wykorzystywane do przenoszenia danych, jak dyski zewnętrzne nie zostały zgubione

- Jeśli zgubiłeś urządzenie, na którym pracujesz lub zostało skradzione natychmiast podejmij odpowiednie kroki, aby o ile to możliwie, zdalnie wyczyścić jego pamięć

EMAIL

- Postępuj zgodnie z obowiązującymi zasadami w organizacji dotyczącymi korzystania ze służbowej poczty elektronicznej (e-mail)

- Używaj przede wszystkim służbowych kont email. Jeśli pracujesz przetwarzając dane osobowe i musisz używać prywatnego e-maila, upewnij się, że treść i załączniki są właściwie szyfrowane. Unikaj używania danych osobowych lub poufnych informacji w temacie wiadomości

- Przed wysłaniem maila upewnij się, że wysyłasz go do właściwego adresata, zwłaszcza jeśli wiadomość zawiera dane osobowe lub dane wrażliwe

- Dokładnie sprawdź nadawcę maila. Nie otwieraj wiadomości od nieznanych adresatów, a zwłaszcza nie otwieraj załączników oraz nie klikaj w link zawarty w takiej wiadomości. To może być atak phishingowy.

- Nie przesyłaj mailem informacji zaszyfrowanej razem z hasłem. Nawet w osobnej wiadomości. Ten kto ma dostęp do Twojej poczty bez problemu odszyfruje wiadomość.

DOSTĘP DO SIECI I CHMURY

- Używaj tylko z zaufanego dostępu do sieci lub chmury oraz przestrzegaj wszelkich zasad i procedur organizacyjnych dotyczących logowania i udostępniania danych

- Jeśli natomiast nie pracujesz w chmurze lub nie masz dostępu do sieci, zadbaj aby przechowywane dane były w bezpieczny sposób zarchiwizowane.

Na podstawie Protecting Personal Data When Working Remotely przygotowanego przez DPC Ireland.