Praca zdalna a ochrona danych osobowych

Kategoria: Polityka Społeczna
Opublikowano: czwartek, 19, marzec 2020 11:42
Katarzyna Liszka-Michałka
Odsłony: 1340

Ponieważ środki kontroli i zapobiegania rozprzestrzenianiu się COVID-19 będą wymagały większej liczby osób pracujących zdalnie niż zwykle Urząd Ochrony Danych Osobowych udostępnił wskazówki dotyczące bezpieczeństwa danych osobowych podczas pracy poza biurem.

O czym więc należy pamiętać pracując na różnego typu urządzeniach?

1. Urządzenia i oprogramowanie przekazane przez pracodawcę do pracy zdalnej służą do wykonywania obowiązków służbowych. Dlatego też należy postępować zgodnie z przyjęta w organizacji procedurą bezpieczeństwa.
2. Nie wolno instalować dodatkowych aplikacji i oprogramowania niezgodnych z procedurą bezpieczeństwa organizacji.
3. Należy upewnić się, że wszystkie urządzenia z jakich korzystamy mają niezbędne aktualizacje systemu operacyjnego (IOS lub Android), oprogramowania oraz systemu antywirusowego.
4. Należy wydzielić sobie odpowiednią przestrzeń, tak aby ewentualne osoby postronne, nie miały dostępu do dokumentów, nad którymi pracujemy. Odchodząc od stanowiska pracy każdorazowo trzeba zablokować urządzenie, na którym pracujemy.
5. Komputer należy zabezpieczyć 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.
6. Należy podjąć szczególne środki, aby urządzenia z których korzystamy podczas pracy, szczególnie te wykorzystywane do przenoszenia danych, jak dyski zewnętrzne nie zostały zgubione.
7. Jeśli urządzenie, na którym pracujemy zostało zgubione lub zostało skradzione natychmiast podejmijmy odpowiednie kroki, aby o ile to możliwie, zdalnie wyczyścić jego pamięć.

Wytyczne dotyczące wysyłania korespondencji e-mail:

1. Postępuj zgodnie z obowiązującymi zasadami w organizacji dotyczącymi korzystania ze służbowej poczty elektronicznej (e-mail).
2. 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.
3. Przed wysłaniem maila upewnij się, że wysyłasz go do właściwego adresata, zwłaszcza jeśli wiadomość zawiera dane osobowe lub dane wrażliwe.
4. 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.

W zakresie dostępu do sieci i chmury UODO zaleca używać tylko z zaufanego dostępu do sieci lub chmury oraz przestrzegania wszelkich zasad i procedur organizacyjnych dotyczących logowania i udostępniania danych. Jeśli natomiast nie pracujemy w chmurze lub nie mamy dostępu do sieci, należy zadbać aby przechowywane dane były w bezpieczny sposób zarchiwizowane.

Źródło: www.uodo.gov.pl

Phoca PDF