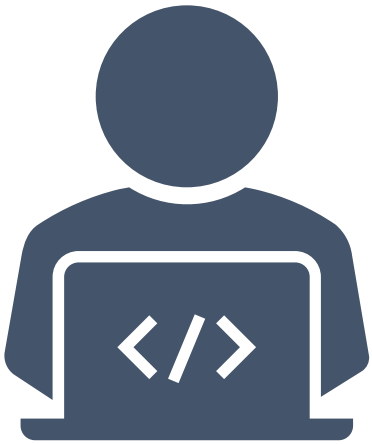
ALERT PRAWNY COVID-19

Zabezpieczenia pracy zdalnej



COVID-19

Zlecając pracownikom pracę zdalną nie można zapominać o wprowadzeniu adekwatnych zabezpieczeń mających na celu zabezpieczyć dane należące do przedsiębiorstwa. W tym alercie prezentujemy listę **17 rozwiązań**, które mogą zwiększyć bezpieczeństwo przetwarzanych przez Państwa danych osobowych.

1. zapewnienie pracownikom urządzeń służbowych, takich jak telefony, laptopy, tablety i zobowiązanie pracowników do niewykorzystywania do pracy sprzętów prywatnych
2. przypomnienie pracownikom o obowiązujących u pracodawcy procedurach bezpieczeństwa korzystania z urządzeń służbowych oraz logowania i udostępniania danych w chmurze
3. zobowiązanie pracowników do niewykorzystywania urządzeń służbowych do celów prywatnych
4. ograniczenie uprawnień użytkowników tak, aby nie mogli samodzielnie instalować nowego oprogramowania
5. stosowane oprogramowanie powinno być automatycznie i regularnie aktualizowane
6. zobowiązanie pracowników do natychmiastowego poinformowania pracodawcy o zgubieniu lub kradzieży urządzeń służbowych (jeśli to możliwe - zdalne usunięcie danych ze sprzętu)
7. wprowadzenie szyfrowania urządzeń przeznaczonych do pracy zdalnej, w tym pendriv'ów
8. wprowadzenie logowania do systemu i poszczególnych programów (np. poczta elektroniczna) przy pomocy loginu i hasła (zaleca się zastosowanie uwierzytelniania dwuskładnikowego)
9. wyłącznie opcji automatycznego logowania i niezapamiętywanie haseł dostępu
10. ustawienie automatycznego blokowania urządzenia po kilkominutowym braku aktywności oraz blokowanie urządzenia przez użytkownika przy każdym odejściu od stanowiska pracy

Kancelaria Ostrowski i Wspólnicy sp. k., ul. Lubicka 53, 87-100 Toruń,
(+48) 724 679 513 ■ torun@ostrowski-legal.net ■ www.ostrowski.legal

11. szyfrowanie treści i załączników wiadomości

12. korzystanie tylko ze służbowych adresów e-mail

13. niezamieszczanie danych osobowych ani informacji poufnych w temacie wiadomości

14. regularne archiwizowanie danych

15. przed wysłaniem należy upewnić się, że wiadomość jest wysyłana do poprawnego adresata, a przed otwarciem, że wiadomość pochodzi z zaufanego źródła

16. nie należy otwierać załączników z wiadomości od nieznanych nadawców

17. logowanie do rozwiązań chmurowych powinno następować tylko, gdy mamy pewność, że połączenie jest bezpieczne, w szczególności nie należy łączyć się do chmury z sieci publicznych

Powyższa lista uwzględnia zabezpieczenia zalecane przez Urząd Ochrony Danych Osobowych. Podejmując decyzję należy jednak pamiętać, że zastosowane środki powinny być dostosowane do sytuacji danego pracodawcy, **nie ma jednej recepty na zapewnienie bezpieczeństwa danych**. Np. korzystanie ze służbowych adresów e-mail, gdy pracownicy nie otrzymają urządzeń służbowych, nie zawsze musi być najlepszym rozwiązaniem. Pracodawca powinien zastanowić się, co będzie w danym wypadku bezpieczniejsze – umożliwienie pracownikowi logowania się do służbowej poczty e-mail na komputerze prywatnym, czy też wykorzystywanie przez pracownika poczty prywatnej w celach komunikacji służbowej. Może się bowiem zdarzyć sytuacja, w której zadania pracownika nie będą wiązały się z przetwarzaniem dużej ilości danych osobowych (np. będzie wykorzystywał tylko imiona, nazwiska i służbowe adresy e-mail współpracowników), a korzystanie ze służbowej poczty na urządzeniu prywatnym rodzi ryzyko uzyskania dostępu przez osoby niepożądane, poprzez zainstalowane na komputerze pracownika złośliwe oprogramowanie, do całej bazy adresów mailowych i innych danych osobowych w tym danych szczególnej kategorii. Wdrażając środki ochrony danych osobowych nie można również zapominać o wymogach wynikających z obowiązujących przepisów prawa pracy, w tym w szczególności dotyczących monitoringu pracowników.

Skontaktuj się z nami w celu uzyskania szerszych informacji na powyższy temat.

Skontaktuj się

Paulina Kużdowicz
aplikant radcowski
Kancelaria Ostrowski i Wspólnicy

727 591 259
p.kuzdowicz@ostrowski-legal.net