Zalecenia dotyczące pracy zdalnej – wskazówki dla pracowników

Wszystkie osoby współpracujące z administratorem danych osobowych (ADO), których model współpracy obejmuje pracę zdalną, zobowiązane są do stosowania poniższych środków bezpieczeństwa.

1. Osoby pracujące zdalnie zobowiązane są do wykonywania swoich obowiązków na sprzęcie służbowym. Za wiedzą i zgodą bezpośredniego przełożonego osoby pracujące zdalnie mogą korzystać z prywatnych komputerów, tabletów, telefonów komórkowych itp. urządzeń.
2. Osoby korzystające z prywatnych komputerów zobowiązane są do stosowania następujących, minimalnych środków bezpieczeństwa:
    1) zaszyfrowanie dysku twardego,
    2) założenie oddzielnego konta użytkownika systemu operacyjnego, przeznaczone jedynie do pracy zdalnej, zabezpieczone loginem i bezpiecznym hasłem (lub inną metodą uwierzytelniania),
    3) wykorzystywanie programu antywirusowego z włączonymi ustawieniami, mającymi na celu bieżącą aktualizację silnika programu i bazy zagrożeń,
    4) wykorzystywanie programu typu firewall,
3. Należy unikać zapisywania plików zawierających dane osobowe bezpośrednio na dysku twardym (np. na Pulpicie, w katalogu Pobrane...). Po skończonym dniu pracy należy:
    1) przenieść te pliki do lokalizacji uzgodnionej z bezpośrednim przełożonym lub informatykiem lub
    2) usunąć te pliki z dysku twardego komputera.
4. Przy pracy na papierowych dokumentach zawierających dane osobowe należy stosować następujące, minimalne środki bezpieczeństwa:
    1) przy drukowaniu dokumentów należy od razu zabierać je z tacy odbiorczej, nie dopuszczając do gromadzenia się wydruków,
    2) dokumenty służbowe należy po godzinach pracy umieszczać w szufladzie, szafce lub szafie zamykanej na klucz,
    3) zbędne dokumenty służbowe powinny być niezwłocznie niszczone w niszczarce (nie mogą być wyrzucane do kosza na śmieci).

5. Osoby korzystające z prywatnych urządzeń przenośnych (telefony komórkowe, tablety, iPady) są zobowiązane do stosowania następujących, minimalnych środków bezpieczeństwa:
    1) zabezpieczenie urządzenia zarówno PIN-em, niezbędnym dla uruchomienia urządzenia, jak i dodatkowym zabezpieczeniem (PIN, hasło, odcisk palca, kształt twarzy itp.) w celu wznowienia pracy na urządzeniu po dłuższym okresie nieaktywności lub zablokowaniu urządzenia,
    2) wykorzystywanie programu antywirusowego z włączonymi ustawieniami, mającymi na celu bieżącą aktualizację silnika programu i bazy zagrożeń.
6. Prywatne urządzenia są przechowywane lub transportowane w sposób nienarażający je na zniszczenie, uszkodzenie, kradzież lub zgubienie.
7. W razie zniszczenia, uszkodzenia, kradzieży lub zgubienia prywatnego urządzenia wykorzystywanego w celach służbowych użytkownik urządzenia zawiadamia o tym informatyka (lub inną wyznaczoną osobę) i postępuje zgodnie z jego wskazówkami.
8. Użytkownik urządzenia prywatnego używa internetu w sposób gwarantujący bezpieczeństwo transmisji, w szczególności poprzez:
    1) wykorzystanie mobilnej transmisji danych z własnego urządzenia,
    2) wykorzystanie mobilnej transmisji danych dla udostępnienia internetu na innym urządzeniu (tethering),
    3) wykorzystanie technologii VPN dla zabezpieczenia publicznie dostępnej sieci wi-fi,
    4) wykorzystywanie godnych zaufania sieci wi-fi.
9. Użytkownik urządzenia nie instaluje na nim żadnych aplikacji, które synchronizują zdjęcia lub inne dokumenty służbowe z prywatnym kontem użytkownika (Dropbox, OneDrive, Dysk Google, iCloud itp.).
10. W sprawach nieuregulowanych użytkownik jest zobowiązany do stosowania:
    1) obowiązującej w ADO dokumentacji RODO,
    2) innych wytycznych, regulaminów lub instrukcji związanych z ochroną danych osobowych lub bezpieczeństwem informacji,
    3) poleceń informatyka, IOD lub bezpośredniego przełożonego.