Praca zdalna zgodna z RODO

Home office, czyli praca zdalna to jedna z najskuteczniejszych broni w walce z koronawirusem.

Ograniczamy potencjalne zagrożenie, a nasza organizacja może dalej sprawnie funkcjonować.

Korzystajmy z tej możliwości, ale zgodnie z RODO.

Czy w RODO znajdują się wytyczne na temat pracy zdalnej?

Na początek dobra informacja - przepisy RODO nie zabraniają nikomu pracy zdalnej! Rozporządzenie nie zawiera szczegółowych instrukcji lub obostrzeń z tym związanych.

Nie znaczy to jednak, że przy delegowaniu zespołu do pracy zdalnej nie powinniśmy brać pod uwagę przepisów RODO.

W toku działania w trybie *home office,* będzie niewątpliwie dochodziło do przetwarzania danych osobowych poza miejscem jej stałego wykonywania. Mogą się pojawić nowe ryzyka i zagrożenia, które nie występują w przypadku pracy w biurze.

Pamiętaj też o tym, że dane osobowe, to nie jedyna wartościowa informacja znajdująca się w zasobach organizacji, w tym na firmowych laptopach czy smartfonach. Równie wartościowe mogą być np. tajemnice przedsiębiorstwa czy inne informacje prawnie chronione. Więcej o tym w kolejnych akapitach.

Które przepisy RODO powinny nas zainteresować?

W mojej opinii będzie ich co najmniej kilka.

Po pierwsze, niezależnie od miejsca, w którym odbywa się praca, należy stosować adekwatne środki zabezpieczeń technicznych i organizacyjnych (art. 32 RODO).

Po drugie, powinniśmy mieć na uwadze ogólne zasady RODO, a zwłaszcza:

1) integralność i poufność (art. 5 ust. 1 lit. f RODO) - w szczególności przetwarzanie powinno odbywać się w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, a administrator powinien zagwarantować ochronę przed ich niedozwolonym lub niezgodnym z prawem użyciem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem,

2) rozliczalność (art. 5 ust. 2 RODO) - administrator powinien być w stanie wykazać, że przestrzega podstawowych zasad RODO, w tym tej wskazanej powyżej, co oznacza, że powinien on dysponować dowodem na to, że przyjęte środki są faktycznie adekwatne i zostały odpowiednio wdrożone.Po trzecie, żeby pracownicy mogli respektować powyższe zasady – potrzebny jest pewien poziom świadomości.

Jak zastosować adekwatne środki zabezpieczeń, jednocześnie zachowując rozliczalność, integralność i poufność?

Poniżej znajduje się propozycja Zespołu Lex Artist dla zgodnych z RODO warunków korzystania z *home office*. Przygotowaliśmy ją z myślą o wszelkich procesach biznesowych, w których wykonywanie pracy zdalnej jest możliwe.

Praca na tzw. szczególnych kategoriach danych (wcześniej: danych wrażliwych), może wymagać podjęcia dodatkowych środków ostrożności.

Służbowy komputer

Poniżej znajduje się lista najczęściej stosowanych i rekomendowanych środków technicznych.

Służbowy komputer przeznaczony do pracy w trybie *home office* spełniać większość z poniższych kryteriów:

1) indywidualny login oraz hasło dostępu do systemu,
2) możliwość łączenia się z Internetem i firmową siecią za pośrednictwem bezpiecznego łącza VPN,
3) wygaszacz ekranu włączający się po kilku minutach bezczynności,
4) aktualny program antywirusowy z firewallem,
5) możliwość automatycznego backupu danych lub ręczna procedura backupowa,
6) nakładki prywatyzujące na ekran minimalizujące ryzyko wglądu w ekran monitora osobom postronnym,
7) warto rozważyć dodanie drugiego składnika uwierzytelniania użytkownika (tzw. 2FA). Aby zalogować się do laptopa użytkownik musi spełnić łącznie dwa warunki:
    a. coś wiedzieć (pamiętać swoje hasło)
    b. coś posiadać (np. smartfona z tokenem aktywacyjnym, czy kartę chipową)
8) obowiązkowo - zaszyfrowany dysk twardy.

Stosowanie wyżej wskazanych środków zapewni w mojej ocenie adekwatny poziom bezpieczeństwa, kiedy pracujemy w trybie *home office*.

Smartfon to też komputer

Nie zapominaj o tym, że w dzisiejszych czasach smartfony dorównują powoli laptopom. Zarówno jeśli chodzi o ich moc obliczeniową, pamięć (a więc i możliwość przechowywania danych osobowych) oraz funkcjonalność.

Służbowe smartfony są dla nas często podstawowym narzędziem do sprawdzania poczty e-mail, a nawet obsługi przeglądarkowych systemów informatycznych zawierających bardzo duże ilości danych osobowych.

Jest on także bardzo bogatą bazą kontaktów Twojej organizacji (pracowników, klientów, kontrahentów).

Smartfon jest też często tzw. drugim faktorem, czyli drugim elementem w dwuskładnikowym uwierzytelnianiu użytkownika. Jeśli np. podczas pracy zdalnej zostanie Ci skradziony smartfon oraz laptop, bardzo zwiększy to ryzyko dostępu do zasobów danych potencjalnym hakerom.

Podobnie jak w przypadku służbowego komputera, smartfon powinien spełniać większość z poniższych kryteriów:

1) obowiązkowo – blokada ekranu. Sama blokada karty SIM PIN-em to zdecydowanie za mało,
2) szyfrowanie danych,
3) możliwość łączenia się z Internetem i firmową siecią za pośrednictwem bezpiecznego łącza VPN,
4) możliwość automatycznego backupu danych,

A co ze świadomością?

Stosowanie w.w. środków zabezpieczających nie pomoże w niczym, jeśli pracownik udostępni włączony komputer osobie trzeciej., albo zostawi go na przednim fotelu auta robiąc zakupy.

Dlatego ważna jest również świadomość pracownika.

W jaki sposób można ją zbudować?

W normalnych warunkach, proponujemy krótkie spotkanie podczas którego pracownik IT przedstawi i opisze zainstalowane środki zabezpieczeń.

Na koniec spotkania wręcz pracownikom oświadczenie, w którym pisemnie zobowiążą się do stosowania w.w. środków.

Jak może wyglądać takie oświadczenie?

Zachęcamy Cię do pobrania edytowalnego szablonu *Oświadczenia w związku z podjęciem pracy zdalnej* (bezpośredni link), który przygotowali nasi eksperci.

Z racji zaistniałej sytuacji, w które możliwość organizacji spotkań jest mocno ograniczona lub zawieszona, najlepszym wyjściem będzie wysłanie maila do wszystkich pracowników o obowiązujących podczas pracy zdalnej zasadach,

Zewnętrzne nośniki danych

Masz pracować zdalnie na dużych pojemnościowo plikach i bazach danych? Chcesz w tym celu skorzystać z zewnętrznego nośnika danych (np. pendrive, zewnętrzny dysk twardy)? Potrzebujesz wykonać backup na zewnętrzny nośnik danych?

Bezwzględnie korzystaj wyłącznie z szyfrowanych nośników danych zgodnych z wewnętrzną procedurą obowiązującą w Twojej organizacji.

Komputer prywatny (BYOD)?

Możemy zezwolić pracownikom na pracę zdalną na własnym sprzęcie komputerowym i zastosować coraz popularniejsze rozwiązanie BYOD (Bring Your Own Device). Taka praktyka nie jest zabroniona przez RODO, musimy jednak pamiętać o kilku bardzo istotnych elementach.

Może się to odbyć wyłącznie za **dobrowolną** zgodą pracownika.

Aby dopuścić prywatny sprzęt do użytku, dział IT powinien wcześniej zadbać o jego odpowiednie zabezpieczenie i sprawdzenie. Przy tej okazji możemy wejść w obszar prywatności naszego pracownika.

Wcześniej wskazane punkty dotyczące sprzętu służbowego odnoszą się również (a wręcz – przede wszystkim) do komputerów prywatnych.

Dokumenty papierowe

Unikaj wynoszenia dokumentów papierowych poza Twoją organizację. W dzisiejszych czasach w większości przypadków możemy pracować na skanach, zdjęciach czy gotowych bazach danych.

Jeśli nie będzie innej możliwości, zadbaj o to, żeby uniemożliwić dostęp do dokumentów osobom nieupoważnionym (w tym domownikom!). . Pamiętaj aby nie wyrzucać dokumentów zawierających dane osobowe do kosza w domu. W razie potrzeby zabierz je po zakończeniu pracy zdalnej do biura, aby zniszczyć je w niszczarce.

Nie tylko dane osobowe są ważne

Dane osobowe nie są jedynymi informacjami, które powinniśmy w należyty sposób chronić. Do innych chronionych danych, mogą należeć również:

1) tajemnica przedsiębiorcy,
2) tajemnica skarbowa,
3) tajemnica telekomunikacyjna,
4) inne tajemnice prawnie chronione (np. lekarska, radcowska, adwokacka etc.)

Jeśli podczas swojej pracy zdalnej, będziesz korzystać nie tylko z danych osobowych ale i innych chronionych informacji, pamiętaj o odpowiednich środkach bezpieczeństwa!

Podsumowanie

Możesz pozwolić pracownikom na pracę zdalną i pozostać w zgodzie z przepisami RODO.

Pamiętaj o kilku opisanych wyżej zasadach. Dzięki nim zminimalizujesz ryzyko naruszenia danych osobowych.

A jeśli już coś złego się wydarzy, to mając wdrożone adekwatne środki – nie powinieneś spodziewać się dodatkowych kłopotów ze strony organu nadzorczego.

Autor artykułu:

Przemysław Zegarek, Prezes Zarządu

Źródła:

- 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)
- Ustawa o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych
- praktyczne doświadczenie budowania systemów ochrony danych osobowych od 2008 roku (jako ABI) i po 2018 roku (jako IOD)