

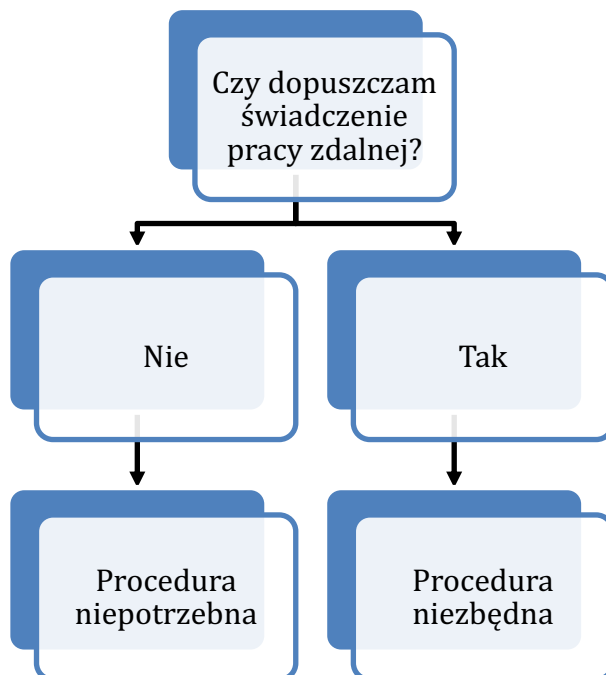
Warszawa, dn. 19.04.2023 r.

Procedura ochrony danych osobowych w pracy zdalnej - kiedy jest potrzebna i jak ją wprowadzić?

Od 07 kwietnia 2023 r. obowiązują znowelizowane przepisy Kodeksu Pracy o świadczeniu pracy zdalnej. Jeżeli firma dopuszcza taką formę świadczenia pracy, zasady ją regulujące powinny w dacie publikacji niniejszego tekstu być już uchwalone i znane pracownikom. Pierwsze miesiące obowiązywania nowych zasad są też doskonałym czasem na weryfikację, czy posiadana dokumentacja jest zgodna z przepisami oraz czy pracownicy prawidłowo ją realizują. Im szybciej firma wychwyci nieprawidłowe praktyki, tym łatwiej będzie je ukrócić – zanim staną się nawykiem.

Kto musi mieć Procedurę ochrony danych osobowych w pracy zdalnej?

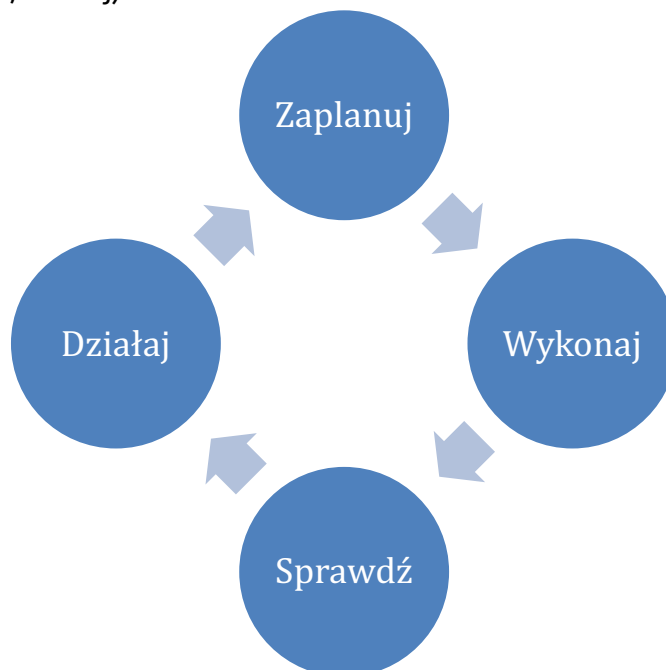
Wielką zaletą (ale czasami też i wadą) RODO jest elastyczność zawartych tam przepisów. Oznacza to niestety, że często odpowiedź na konkretne pytania o ochronę danych osobowych brzmi „to zależy”. W sprawie zasad ochrony danych osobowych w pracy zdalnej sytuacja jest na szczęście niezwykle prosta. Pracodawca musi bowiem zadać sobie tylko jedno proste pytanie:



Przepis art. 67²⁶ ust. 1 Kodeksu pracy jest w tym zakresie jednoznaczny: *na potrzeby wykonywania pracy zdalnej pracodawca określa procedury ochrony danych osobowych oraz przeprowadza, w miarę potrzeby, instruktaż i szkolenie w tym zakresie*. Czytając go łącznie z art. 5 ust. 2 RODO (zasada rozliczalności) nie mamy wątpliwości: Pracodawca musi nie tylko wdrożyć zasady ochrony danych osobowych w pracy zdalnej w swojej organizacji, ale również móc wykazać, że zapoznał z tymi zasadami pracowników, a nadto zapewnił im instruktaż i szkolenie.

Jak opracować Procedurę?

Choć najprostszym rozwiązaniem może wydawać się pobranie darmowego wzoru dokumentu z Internetu, zmiana w nim nazwy firmy i rozesłanie go do pracowników, zdecydowanie lepszym (tak w krótkim, jak i w długim okresie) rozwiązaniem jest systematyczne podejście do sprawy i przygotowanie dokumentacji „uszytej na miarę” dla organizacji. Jak to zrobić? Niezwykle pomocny w uporządkowanym podejściu do tego typu działań jest tzw. Cykl Deminga („PDCA” od angielskiego: Plan, Do, Check, Act, czyli Zaplanuj, Wykonaj, Sprawdź, Działaj).



Choć metoda ta jest immanentnie wpisana w metodykę zarządzania wynikającą z norm ISO, warto z niej skorzystać również w sytuacji, gdy organizacja nie wdrożyła systemów zarządzania opartych na normach z tej serii.

Zaplanuj

Pierwszym krokiem powinno być zebranie rzetelnych i aktualnych informacji o własnej organizacji. Jakie dane i gdzie przetwarzamy? Czy wiążą nas jakieś dodatkowe wymogi (tzw. otoczenie regulacyjne – a więc wdrożone standardy jak ISO 9001, czy ISO 27001, ale również podpisane z kontrahentami i klientami umowy, które mogą zawierać dodatkowe obowiązki w zakresie postępowania z danymi). Na jakim sprzęcie pracujemy? Jakie stosujemy zabezpieczenia techniczne (połączenia VPN, autoryzacja dwuskładnikowa, itp.)? W zgromadzeniu tych informacji pomogą nam poszczególne komórki w organizacji – Inspektor Ochrony Danych (IOD), Dział IT, Dział Prawny, HR, administracja, sprzedaż... Na tym etapie ustalimy, jakie dane będą przetwarzane w pracy zdalnej, kto będzie z dokumentu korzystał, jakie wymogi muszą się w nim znaleźć oraz jakie inne działania będą konieczne dla realizacji procesu (np. aneksowanie niektórych umów, przeprowadzenie DPIA, pozyskanie dodatkowych zabezpieczeń technicznych, itp.). Wiedząc to, możemy przygotować dokument procedury.

Co powinno znaleźć się w procedurze?

Obowiązujące przepisy nie zawierają listy zagadnień, które powinny zostać uregulowane w procedurze ochrony danych osobowych przy pracy zdalnej. Istotne jest zawarcie tu konkretnych zapisów, które pozwolą na ochronę informacji przedsiębiorcy. Dotyczy to nie tylko informacji stanowiących dane osobowe. Truizmem będzie powiedzieć, że wyciek informacji nie będących danymi osobowymi, takich jak np. dane księgowo czy informacje o procesach technologicznych, również może być bardzo niebezpieczny dla organizacji. Co dokładnie powinno znaleźć się w dokumencie, zgrabnie opisała [Nina Zacharska](#) na naszym Blogu miesiąc przed wejściem w życie nowelizacji Kodeksu Pracy.

Wykonaj

Mamy gotowy dokument. Co dalej? Kolejnym krokiem jest oczywiście wdrożenie go w organizacji i zakomunikowanie zmiany pracownikom. Zgodnie z obowiązującymi zasadami może to być uchwała zarządu, uchwała wspólników, czy decyzja właściciela firmy. Wszyscy pracownicy muszą zapoznać się z dokumentem, podpisać stosowne oświadczenia, wziąć udział w omówieniu nowych zasad, czy szkoleniu. Należy dopilnować, by pracownicy dysponowali stosownym sprzętem, oprogramowaniem i wsparciem. Wszystkie te działania również należy udokumentować – pozwoli to nie tylko na wykazanie zgodności w razie kontroli realizowanej przez Urząd Ochrony Danych Osobowych, ale również dodatkowo zmotywuje pracowników do przestrzegania nowych zasad.

Sprawdź

Częstym błędem na polskim rynku (i to nie tylko w zakresie ochrony danych osobowych) jest opracowanie jakiejś dokumentacji „na wypadek kontroli” i pozostawienie jej w szufladzie, wyłącznie na tę okoliczność. To ogromny błąd. Dobre i przemyślane zasady ochrony danych osobowych nie tylko pozwolą uniknąć kary, ale stanowią dużą wartość dodaną dla organizacji. Korzyści te można osiągnąć jednak tylko wtedy, gdy zasady te stosujemy, a następnie uzupełniamy i korygujemy. Kontrola znajomości i przestrzegania nowych zasad pozwoli nie tylko zweryfikować, czy nowe zasady są przestrzegane (co przełoży się na mniejszą ilość incydentów ochrony danych), ale również wychwycić ewentualne luki, czy nadmiarowe zapisy we wdrożonych dokumentach. Może ktoś nie był na szkoleniu z powodu choroby lub urlopu?

Działaj

Przedsiębiorca, uzbrojony w wiedzę o ewentualnych uchybieniach w organizacji, może niezwłocznie je skorygować – zanim złe praktyki wejdą w nawyk i doprowadzą do wystąpienia incydentów. Oznacza to oczywiście (w miarę stwierdzonych potrzeb) uzupełnienie lub zmianę procedury, dodatkowe szkolenia, itp.

Daniel Taberski – radca prawny, specjalista ds. ochrony danych w iSecure Sp. z o.o.