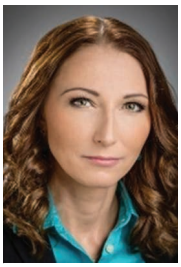
Jak chronić dane w obliczu konieczności zdalnego trybu pracy?

How to protect data in the face of remote operation?



Marlena Wach

Dr, Radca Prawny

Kancelaria J. Bójko i Wspólnicy („JBW")

m.wach@kancelariajbw.com.pl

Streszczenie: Obecna sytuacja epidemiologiczna odznacza piętno na przedsiębiorcach, stawiając przed nimi wyzwania związane z zachowaniem ciągłości działalności. W poprzednich artykułach dotyczących ochrony danych osobowych skupiliśmy się m.in. na obniżeniu ekspozycji biologicznej pracowników czy też ochronie danych osobowych w ramach gromadzenia przez przedsiębiorców danych medycznych pracowników i klientów/potencjalnych klientów przedsiębiorstw. Aspekty te koncentrują się jednak na sytuacjach, w których obecność pracowników w zakładach pracy jest niezbędna. Jak więc wygląda sytuacja ochrony danych w przypadku podmiotów, w których istnieje możliwość przeniesienia całości lub jakiejś części ich działalności na tryb zdalny oraz jakich zasad należy przestrzegać?

Słowa kluczowe: *Zdalny tryb pracy; Epidemia; Przedsiębiorstwo*

Abstract: The current epidemiological situation has a stigma on entrepreneurs, posing challenges related to maintaining business continuity. In previous articles on the protection of personal data, we focused, among others on the reduction of biological exposure of employees or the protection of personal data as part of the collection of medical data of employees and customers / potential customers of enterprises by entrepreneurs. However, these aspects focus on situations where the presence of employees in workplaces is essential. So what is the data protection situation for entities in which it is possible to transfer all or some part of their activities to remote mode and what rules should be followed?

Keywords: *Remote operation mode; Epidemic; Undertaking*

Duży odsetek przedsiębiorstw ma możliwości i instrumenty pozwalające na dostosowanie świadczonych przez siebie usług do trybu zdalnego. Zdalny charakter pracy niesie za sobą jednak konieczność przestrzegania kilku procedur w celu zapewnienia jak najwyższego bezpieczeństwa podczas realizowania zadań pracowniczych oraz płynnego prowadzenia działalności przez przedsiębiorców. W zakresie ochrony danych osobowych podczas pracy zdalnej UODO w komunikacie z dnia 17 marca 2020 r. wskazuje m.in. na następujące czynności pozwalające na zachowanie bezpieczeństwa danych osobowych podczas pracy poza biurem w zakresie:

a) Urządzeń:

- Postępowanie zgodnie z procedurą bezpieczeństwa w zakresie pracy na urządzeniach i z wykorzystaniem oprogramowania przekazanego przez pracodawcę;
- Nieinstalowanie dodatkowych aplikacji i oprogramowania;
- Zapewnienie niezbędnych aktualizacji systemów operacyjnych, oprogramowania oraz systemów antywirusowych;
- Odpowiednie przechowywane dokumentacji oraz uniemożliwienie dostępu do niej osobom trzecim;
- Każdorazowe wylogowanie się z platform służbowych po zakończeniu pracy;
- Zachowanie szczególnych środków bezpieczeństwa, zabezpieczanie sprzętu oraz wykorzystywanych platform silnymi hasłami dostępu;
- Podjęcie szczególnych środków zabezpieczających wykorzystywane do pracy zdalnej urządzenia przed zgubieniem lub kradzieżą oraz niezwłoczne poinformowanie pracodawcy w przypadku zaistnienia takiego zdarzenia (w tym także podjęcie kroków w celu zdalnego wyczyszczenia pamięci urządzenia – o ile to możliwe).

b) Skrzynek e-mail:

- Postępowanie zgodnie z procedurą bezpieczeństwa w zakresie korzystania ze służbowej poczty elektronicznej;
- Używanie przede wszystkim służbowych kont e-mail, w przypadku zaistnienia konieczności korzystania z prywatnej poczty elektronicznej należy upewnić się, iż

treści, załączniki są odpowiednio szyfrowane;
- Dołożenie wszelkich starań, aby korespondencja zawsze trafiała do właściwego adresata;
- Wstrzymanie się od otwierania wiadomości mailowych od nieznanych adresatów, załączników oraz linków w takich wiadomościach;
- Wysyłanie zaszyfrowanej wiadomości i hasła odszyfrowującego różnymi metodami;

c) Dostępu do sieci i chmury:

- Korzystanie z sieci i usług chmurowych tylko z zaufanych źródeł, a także przestrzeganie wszelkich zasad i procedur organizacyjnych dotyczących logowania i udostępniania danych;
- Odpowiednia archiwizacja i przechowywanie danych w przypadku braku możliwości pracy w chmurze lub w przypadku braku dostępu do sieci.

Regulamin pracy zdalnej

Warto zrobić inwentaryzację, co może być przeniesione w tryb zdalny, a jakie czynności muszą pozostać w trybie wykonywania ich osobiście w biurze lub w terenie, zakładzie oraz czy te ostatnie nie wymagają przeorganizowania i dostosowania do sytuacji. Przenosząc biuro w tryb zdalny należy także zastanowić się, czy rzeczywiście wszystko trzeba przenieść, do jakich dokumentów pracownik musi mieć dostęp, jak je ma archiwizować (czy ma je niszczyć a jeżeli tak to w jaki sposób). Te oraz inne informacje powinny się znaleźć w Regulaminie pracy zdalnej lub innym dokumencie wdrażającym wiążące reguły pracy zdalnej. Regulamin ten może określać spotkania online z pracownikami o ustalonych porach rano i po południu oraz metody rejestrowania czasu pracy, pokazywania swojej aktywności. Może też pracodawca może wyposażyć pracowników w zamykane skrzynki, tak aby po zakończeniu pracy mogli oni złożyć do nich dokumenty, aby przez przypadek nie uległy one zalaniu lub zniszczeniu w tzw. środowisku home office. Pod względem ochrony danych osobowych pracodawca powinien wykonać analizę przetwarzania danych, czy na przykład w nowych okolicznościach nie przetwarzane są dodatkowe dane osobowe albo w inny sposób, czy udostępnianie są dane do krajów trzecich. Warto także przeszkolić pracowników w zakresie nowego regulaminu czy procedury regulujące pracę zdalną, gdyż w nowym środowisku pracy domowej łatwo o nieuwagę i przesłanie np. poufnej informacji do niewłaściwego adresata i w zależności od zawartości może stanowić to incydent w zakresie bezpieczeństwa danych.

Organizacja pracy zdalnej wymaga uregulowanie jej w polityce lub regulaminie

Obecna sytuacja, gdy WHO ogłosiło na świecie stan pandemii, a polski rząd wprowadził stan zagrożenia epidemicznego i zamknął polskie granice, wpływa niewątpliwie na organizację pracy w przedsiębiorstwie. Obywatele zobowiązani zostali wydanymi przez Rząd aktami prawnymi do pozostania w domu [1]. Wymusiło to na przedsiębiorcach szukania rozwiązań w pracy zdalnej w celu możliwości kontynuowania działalności. Brak odpowiedniego dostosowania się do aktualnej sytuacji, może doprowadzić do wielu negatywnych konsekwencji dla przedsiębiorców.

Przygotowanie przedsiębiorcy do pracy zdalnej

Analizy wymaga, czy ze względu na świadczone usługi, dostarczane towary i całościowy zakres działalności danego przedsiębiorcy istnieje możliwość całościowego przeniesienia wykonywania pracy w tryb zdalny, a jeżeli nie, to w jakiej części. Jakie procesy i działania mogą odbywać się w trybie zdalnym a jakie muszą nadal być obsługiwane z biura. Dobrze jest zrobić inwentaryzację wewnątrz organizacji angażując osoby z działu IT, osoby zarządzające zespołami oraz uwzględnić działania, które muszą być podjęte w stosunku do pracowników. Powyższa mapa procesów i czynności musi być konsultowana z inspektorem ochrony danych (IOD) lub z osobą nadzorującą kwestie ochrony danych i bezpieczeństwa w podmiocie. IOD powinien być włączony w te procesy od samego początku.

Inwentaryzacja sprzętowa

Dział odpowiedzialny za sprzęt, urządzenia, narzędzia, którym jest zwykle dział IT powinien sprawdzić ile, jakim sprzętem oraz oprogramowaniem dysponuje, czy nie należy zakupić nowego sprzętu i wyposażyć go w aktualne oprogramowanie. Weryfikacji wymaga, czy zainstalowane są na urządzeniach narzędzia monitorujące i zabezpieczające dane oraz czy zapewnione jest wsparcie techniczne. Przedsiębiorca może rozważyć, czy dopuści możliwość korzystania przez pracownika z własnego, prywatnego sprzętu, tzw. Bring Your Own Device (BYOD) [2]. Wydane narzędzia powinny być sprawdzone pod względem technicznym. Warto także sprawdzić, czy potrzebujemy jakiś narzędzi, np. do rejestracji czasu pracy i organizacji pracy zdalnej lub spotkań online, a obecnie tych narzędzi nie mamy. Wówczas należałoby zastanowić się, jakie narzędzia nam są potrzebne i je zakupić instalując także to oprogramowanie na urządzeniach.

Regulamin lub polityka pracy zdalnej

Przedsiębiorca powinien także zweryfikować obowiązujące polityki, instrukcje, regulaminy i wprowadzić jako ich uzupełnienie lub jako nowy dokument, regulamin czy politykę pracy zdalnej (lub zaktualizować już obowiązujący). Musimy uzyskać pew-

ność i rozliczalność: ewidencja wydanego sprzętu, protokoły zdawczo-odbiorcze, ewidencje zaświadczeń i oświadczeń.

1) Obowiązki pracownika

Regulamin taki powinien określać obowiązki pracownika nie tylko w zakresie przestrzegania obowiązujących u pracodawcy polityk, procedur i instrukcji ale także pozostawania do dyspozycji pracodawcy w ustalonych godzinach pracy i pozostawania z nim w stałym kontakcie za pomocą uzgodnionych środków łączności.

Warto uzgodnić sposób komunikacji oraz w jaki sposób wykazywana będzie aktywność pracownika, stałe godziny wspólnych spotkań, np. 10 i 15. Pracownik powinien być zobowiązanych do bieżącego informowania o wynikach i efektach swojej pracy oraz właściwego korzystania z powierzonego sprzętu służbowego. Także do natychmiastowego zgłaszania pracodawcy przeszkód w wykonywaniu pracy z domu, w szczególności awarii urządzeń. Pracodawca powinien mieć także prawo przeprowadzenia kontroli, czy pracownik wykonuje rzeczywiście powierzoną mu pracę. Warto określić także sposoby przekazywania i weryfikacji poleceń, jak wykazujemy aktywność, że jesteśmy dostępni

2) Obszar techniczny

Dobrze, aby pracodawca po dokonaniu przeglądu narzędzi oraz oprogramowania, identyfikacji nowych narzędzi i rozwiązań, które trzeba zakupić, np. do zarządzania projektami online czy też rejestru czasu pracy, ustalił także listę dopuszczalnego oprogramowania oraz tych, których nie można instalować, bo są nie autoryzowane. W regulaminie powinny się znaleźć ustalenia w zakresie wykorzystywania urządzeń, skrzynki e-mail oraz sieci i chmury.

a) Urządzenia: wykorzystywane oprogramowanie dostarczone oraz rekomendowane przez pracodawcę (lista autoryzowanego oprogramowania) oraz zakaz instalowania nie autoryzowanego oprogramowania, wykonywanie niezbędnych aktualizacji systemów operacyjnych, oprogramowania oraz systemów antywirusowych. Dokumentacja czy to papierowa, czy elektroniczna, powinna być zabezpieczona a dostęp do niej mogą mieć tylko osoby upoważnione. Pracownik powinien się każdorazowo wylogowywać się z platform służbowych po zakończeniem pracy i włączać zabezpieczenie ekranu za każdym razem, gdy ma przerwę lub nie ma go w pobliżu komputera, stosowane także powinny być silne hasła dostępu, a urządzenia zabezpieczone przed zgubieniem lub kradzieżą oraz wprowadzony obowiązek niezwłocznego poinformowania pracodawcy w przypadku zaistnienia takiego zdarzenia, w tym także podjęcie kroków w celu zdalnego wyczyszczenia pamięci urządzenia – o ile to możliwe. Wprowadzenie zakazu udostępnianie sprzętu służbowego członkom rodziny, zasad w zakresie zgłaszania awarii, kwestii dopuszczalności korzystania z nośników zewnętrznych.

b) Skrzynki e-mail: używanie przede wszystkim służbowych kont e-mail, sprawdzanie właściwych adresatów, załączników, szyfrowanie treści, załączników, nie otwieranie wiadomości mailowych od nieznanych adresatów, załączników oraz linków w takich wiadomościach, wysyłanie zaszyfrowanej wiadomości i hasła odszyfrowującego różnymi metodami. Przyprowadzenie szkolenia uczulającego pracowników na różne metody wyłudzenia informacji.

c) Dostępu do sieci i chmury: korzystanie z sieci i usług chmurowych ze zweryfikowanych źródeł, przestrzeganie zasad bezpieczeństwa w zakresie logowania i udostępniania danych, udostępnianie materiałów w postaci screen sharing tylko osobom uprawnionym. Weryfikacja sposobu łączenia się do sieci i wybór bezpiecznego łącza, korzystanie z VPN.

3) Obszar organizacyjny, dokumentacja

Analiza, czy wszystkie urządzenia oraz dokumenty potrzebne są w celu wykonywania pracy zdalnej, czy część z nich może pozostać w biurze, wprowadzenie ewidencji wydanej dokumentacji. Pracodawca także powinien uregulować sposób, w jaki przekazywana jest pracownikom, wydawana, dokumentacja papierowa (gdy nie da się jej zamienić na formę elektroniczną), czy jest to wewnętrzna dokumentacja przedsiębiorstwa czy dokumentacja klienta, jak następnie archiwizowana i czy ma być niszczona przez pracownika, czy przechowywana i przekazywana do biura w momencie powrotu do pracy lub przez kuriera. Pracodawca może wyposażyć pracowników w zamykane skrzynki, pojemniki, teczki, tak aby po zakończeniu pracy mogli oni włożyć do nich dokumenty papierowe, aby przez przypadek nie uległy one zalaniu lub zniszczeniu w tzw. środowisku home office. Wykorzystanie narzędzi do rozdzielania, rozliczenia zadań, czasu i efektów pracy oraz weryfikacji wykonanej pracy.

Stałe dyżury w biurze

Czy konieczne jest ustalenie stałego dyżuru w biurze oraz wyznaczenie pracownika, który zajmuje się obiegiem papierowych dokumentów oraz obsługą incydentów. Gdy jest konieczne utrzymanie biura stacjonarnego, powinny zostać zaktualizowane procedury pracy zespołu wsparcia oraz dyżury. Analogicznie powinno być uregulowane także, w jaki sposób przechowywana jest dokumentacja elektroniczna oraz archiwizowana, zarządzanie kopiami zapasowymi, uregulowanie czy i kiedy będą one wykonywane. Nie można także zapomnieć o zabezpieczeniu biura stacjonarnego, pomieszczeń, sprzętu, kluczy. Personel powinien otrzymać gotowe instrukcje, zasady jak zabezpieczać dokumenta-

cje, stację roboczą, stanowisko pracy, klucze i kart dostępu.

Dopuszczenie używania sprzętu prywatnego pracowników

Pracodawca może także rozważyć umożliwienie dopuszczenia wykorzystywania sprzętu prywatnego pracowników do celów służbowych (Bring Your Own Device (BYOD) zwłaszcza w sytuacji, kiedy nie dysponuje odpowiednią ilością urządzeń przenośnych z których pracownik mógłby korzystać w domu. Pracodawca powinien wprowadzić oprogramowanie zabezpieczające, które powinno być zainstalowane na tym urządzeniu prywatnym oraz wprowadzić autoryzację, korzystanie z VPN, hasła i blokady ekranów oraz analogiczne zabezpieczenia o których wspomniane zostało już powyżej. Ponadto rozdzielność dokumentów, danych służbowych oraz prywatnych, zakaz korzystania ze korzystania ze skrzynki służbowej do celów prywatnych, otwierania określonych aplikacji podczas używania narzędzi służbowych. Konieczność instalowania aktualizacji oprogramowania. Pracodawca zobowiązany jest do ochrony informacji poufnych, danych osobowych oraz informacji osób trzecich, klientów ale także to do wyważenia tego z ochroną prywatności i prywatnych informacji pracownika.

Obowiązki osoby odpowiedzialnej za ochronę danych osobowych

Analizy wymaga, czy nowe narzędzia albo dotychczasowe ale wykorzystywane w inny sposób nie zbierają, przetwarzają dodatkowych danych osobowych np. prywatnego emaila lub adresu IP pracownika czy też lokalizacji miejsca zamieszkania oraz czy nie wysyłane są dane poza Europejski Obszar Gospodarczy. Czy nie pojawiły się dodatkowe zagrożenia, ryzyka dla ochrony danych osobowych związane z pracą zdalną.

Pod względem ochrony danych osobowych pracodawca powinien przeprowadzić analizę ryzyka w związku z organizacją pracy zdalnej i przygotować ocenę skutków dla ochrony danych osobowych.

Istnieje podwyższone ryzyko wystąpienia incydentów i naruszeń podczas pracy zdalnej w zakresie m.in. błędów podczas wysyłania emalii do dużej grupy odbiorców (odkryte emaile); załączenia błędnego pliku do wiadomości email; udostępnienie screenu ekranu komputera; nie stosowanie hasłowania załączników; udostępnienie danych osobowych w postaci wizerunku osób; stania się ofiarą wyłudzenia danych; zainfekowania komputera szkodliwym oprogramowaniem; udostępniania informacji w social media.

Pojawiły się także zapewne nowe procesy, które należy wprowadzić do Rejestru Czynności Przetwarzania (RCP). Przeanalizowania wymaga zakres wydanych upoważnień do przetwarzania danych i ich aktualizacja oraz aktualizacja procedury zgłaszania incydentów bezpieczeństwa danych w przypadku przeniesienia tego procesu w tryb zdalny. Administrator danych ma ciągle tylko 72h na przesłanie zgłoszenia naruszenia danych osobowych do organu regulacyjnego (Prezes UODO).

Szkolenia online

Z uwagi na istotną zmianę w zakresie sposobu przetwarzania danych oraz narzędzi i wprowadzenie dodatkowych polityk regulujących pracę zdalną oraz autoryzowane aplikacje, narzędzia i zaktualizowanie zasad bezpieczeństwa, należy także przeprowadzić szkolenie np. w formie e-learningu. Warto także przeszkolić pracowników w zakresie nowej procedury regulującej pracę zdalną, gdyż w nowym środowisku pracy domowej łatwo o nieuwagę i przesłanie np. poufnej informacji do niewłaściwego adresata i w zależności od zawartości może stanowić to incydent w zakresie bezpieczeństwa danych.

W sytuacji, gdy w wielu przypadkach praca zdalna została wymuszona i niektóre osoby korzystają pierwszy raz z tego rodzaju rozwiązań albo też niektóre procesy zostały przeniesione w tryb zdalny w którym wcześniej nie były realizowane, łatwo o pomyłki zwłaszcza w sytuacjach stresujących, ale także następuje nasilenie się ataków cyberbezpieczeństwa, częstsze próby wyłudzenia informacji oraz podszywania się pod inną osobę lub podmiot. W związku z tym należy zdecydowanie uczulić pracowników na tego rodzaju sytuacje, dzielenie się poufnymi informacjami podczas szkoleń online czy w social media. Uświadomienie o nasilających się zwłaszcza w czasach kryzysu zagrożeniach.◀

Materiały źródłowe

[1] Dnia 28 lutego 2020 r. zakażenie koronawirusem zostało objęte przepisami ustawy z 5 grudnia 2008 r. o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi. Od 8 marca 2020 r. obowiązuje Ustawa COVID-19. Od 14 marca 2020 r. do odwołania na obszarze całego kraju został ogłoszony stan zagrożenia epidemicznego w związku z zakażeniami koronawirusem. Rozporządzenie Ministra Zdrowia z 13 marca 2020 r. w sprawie ogłoszenia na obszarze Rzeczypospolitej Polskiej stanu zagrożenia epidemicznego. Rozporządzenie Ministra Zdrowia z 14 marca 2020 r. zmieniające rozporządzenie w sprawie ogłoszenia na obszarze Rzeczypospolitej Polskiej stanu zagrożenia epidemicznego.

[2] Ustawa o wzajemnych obowiązkach pracodawcy i pracownika pracującego na sprzęcie prywatnym (telepracownika). Regulamin wykonywania pracy w miejscu zamieszkania pracownika przy pomocy urządzeń elektronicznych. Instrukcja bezpieczeństwa i higieny pracy wykonywanej przy pomocy urządzeń elektronicznych w miejscu zamieszkania.