PRACA ZDALNA PO PANDEMII – Raport podsumowujący webinarium #3
Bezpieczeństwo informacji i ochrona danych w kontekście pracy zdalnej

- **Praca zdalna zyskała na znaczeniu podczas pandemii, wciąż jednak wiele branż kontynuuje świadczenie pracy w tej formie. Wiele wskazuje na to, że praca zdalna w kolejnych latach pozostanie jedną z podstawowych form wykonywania obowiązków służbowych.**
- **W Parlamencie trwają prace nad nowelizacją *Kodeksu pracy* wprowadzającą regulacje dotyczące pracy zdalnej. Nowe przepisy zaczną obowiązywać 2023 roku.**
- **Administrator danych ma obowiązek prowadzenia regularnych analiz ryzyka związanego z przestrzeganiem procedur bezpieczeństwa danych podczas wykonywania pracy w formule zdalnej.**
- **Komunikacja w przedsiębiorstwie, instytucji czy organizacji w ramach pracy zdalnej odbywać powinna się bezpiecznymi kanałami służbowymi. Niedopuszczalne jest wykorzystywanie do celów komunikacyjnych prywatnych skrzynek poczty elektronicznej, prywatnych komunikatorów czy sprzętu, nie będącego sprzętem służbowym.**
- **Eksperci z zakresu ochrony danych podkreślają, że potencjalnie niebezpiecznym działaniem może być niewłaściwe korzystanie z dokumentacji papierowej w kontekście pracy zdalnej. Zaleca się regularne niszczenie zbędnych drukowanych dokumentów lub przechowywanie ich w bezpiecznym, przeznaczonym do tego celu, miejscu.**

Związek Przedsiębiorców i Pracodawców, w ramach projektu *Potrzeby i wyzwania związane z wdrożeniem w przedsiębiorstwach prywatnych modelu pracy zdalnej* dofinansowanego z Europejskiego Funduszu Społecznego zlecił zrealizowanie badania *Oczekiwania, potrzeby i postawy pracowników dotyczące pracy zdalnej*.

Praca zdalna zyskała na znaczeniu w okresie pandemii koronawirusa, choć wiele przedsiębiorstw wykorzystywało związane z nią możliwości jeszcze przed rokiem 2020. Szczególnym przypadkiem są tu branże IT oraz e-commerce, w których praca zdalna była i jest

pożądana przez pracowników, co spotyka się często z pozytywnym odbiorem ze strony pracodawców. Faktem jest – co w webinariach organizowanych przez Związek Przedsiębiorców i Pracodawców podkreślali przedstawiciele firm reprezentujących wspomniane branże – że praca zdalna, w wielu przypadkach, stała się dla nich jedną z podstawowych form świadczenia pracy.

Co istotne co szósty badany chcący pracować w formule zdalnej jest skłonny rozważyć zmianę pracodawcy, a aż 47 procent jest gotowe przekwalifikować się, jeśli miałoby wiązać się to z uzyskaniem lepszych warunków pracy zdalnej. Sytuacja jest jednak szczególna w odniesieniu do specjalistów z branży IT. Z badania zrealizowanego przez No Fluff Jobs wynika, że (dane z czerwca 2022 r.) aż 74,6 procenta specjalistów branży IT w Polsce pracuje wyłącznie zdalnie, a 96 procent z nich nie chce wracać do formuły pracy stacjonarnej. Aż 56 procent respondentów wskazało, że w przypadku braku możliwości kontynuowania pracy w formule zdalnej, gotowych jest do zmiany miejsca zatrudnienia na takie, które nie będzie wymagało stałej obecności w biurze. Dane te w odniesieniu do pracy hybrydowej również nie pozostawiają pracodawcom pola manewru – aż 55 procent badanych zadeklarowało bowiem, że nawet w przypadku przejścia z pracy zdalnej na formułę hybrydową będzie szukać nowego miejsca pracy.

To zatem branża IT – choć nie tylko ona, ale także wszelkie inne rodzaje działalności wykorzystujące model zdalny – powinna być szczególnie zainteresowana wdrażaniem i doskonaleniem procedur dotyczących bezpieczeństwa informacji i ochrony danych. Będzie to szczególnie ważne już od 2023 roku, kiedy to w życie wejdzie nowelizacja *Kodeksu pracy* regulująca kwestie związane z pracą zdalną.

Prawne novum

Sejm RP przyjął nowelizację *Kodeksu pracy* wprowadzającą regulacje dotyczące pracy zdalnej. W myśl przepisów, które wejdą w życie już w 2023 roku możliwość prowadzenia pracy zdalnej będzie mogła zostać określona zarówno przy zawieraniu umowy jak i podczas trwania okresu zatrudnienia. Pracownik będzie miał także prawo zawnioskowania o wykonywanie pracy

zdalnej w formie okazjonalnej. Pracodawca, poza szczególnymi przypadkami, nie będzie mógł odmówić wykonywania pracy zdalnej pracownikowi w ciąży, rodzicom dzieci do 4. życia lub wymagającym szczególnej opieki w myśl zasad określonych w ustawie, czy osobom sprawującym opiekę nad innymi członkami rodziny lub osobą pozostającą we wspólnym gospodarstwie domowym posiadającą orzeczenie o niepełnosprawności lub orzeczenie o znacznym stopniu niepełnosprawności.

W myśl nowych przepisów pracodawca będzie zobowiązany do zapewnienia pracownikowi: niezbędnych do wykonywania pracy w formule zdalnej materiałów i narzędzi; serwisu i konserwacji narzędzia pracy; pokrycia wyszczególnionych w ustawie kosztów związanych z wykonywaniem pracy zdalnej czy szkoleń i pomocy technicznej. Pracodawca zyska także możliwość skontrolowania pracy zdalnej, przy założeniu, że kontrola ta nie naruszy prywatności pracownika.

Kierunek zmian w prawie, zmierzający do maksymalnego dookreślenia zasad rządzących pracą zdalną, każe myśleć o tej formie świadczenia pracy jako o formule długookresowej. Pociąga to za sobą konieczność wykreowania procedur dotyczących bezpieczeństwa informacyjnego i ochrony danych.

Przetwarzanie danych osobowych, a praca zdalna

Podstawowym zadaniem administratora, którym w tym przypadku może być na przykład pracodawca, polega na wdrożeniu środków technicznych zgodnych z RODO. Muszą one uwzględniać charakter, zakres i cel przetwarzania oraz uwzględniać ryzyka. Ważnym zdaniem z punkt widzenia administratora danych jest tu bieżąca aktualizacja, która swoim zasięgiem obejmować powinna analizę ryzyka związaną choćby ze zmianą formy wykonywania pracy – tak jak miało to miejsce w przypadku pracy zdalnej.

Jak pokazuje praktyka, wiele procedur dotyczących organizacji pracy zdalnej, z uwagi na dynamiczny rozwój pandemii, wdrażanych było bez dokonania właściwych analiz problematyki bezpieczeństwa informacji i ochrony danych. Doświadczenia przedsiębiorców

na tym polu wielokrotnie wskazywały na realną zmianę sposobów przetwarzania danych i na wykorzystywanie do tego nowych narzędzi. Praca zdalna wymusiła na pracownikach szybkie zaadaptowanie do realizacji zadań środowiska zewnętrznego i nowych narzędzi wymiany plików czy choćby aplikacji służących celom komunikacyjnym.

Dziś przedsiębiorstwa czy instytucje, które wdrożyły model pracy zdalnej, postanowiły nadal wykorzystywać go do realizacji zadań, czy dopiero planują jego zaimplementowanie, stoją w obliczu obowiązku przeprowadzenia procesu weryfikacji ryzyka, którego następstwem powinien być dobór właściwych narzędzi technicznych i organizacyjnych celem zapewnienia bezpieczeństwa informacji i ochrony danych.

Komunikacja i gromadzenie danych, a bezpieczeństwo informacji i ochrona danych w kontekście pracy zdalnej

Komunikacja to podstawowy element, który brany powinien być w kontekście bezpieczeństwa informacji i ochrony danych. Komunikowanie się w ramach przedsiębiorstw, organizacji czy instytucji przy zachowaniu minimum ryzyka to dziś wyzwanie dla wielu podmiotów. O ile w warunkach pracy stacjonarnej, kontakt z administratorem czy osobami odpowiedzialnymi za wsparcie techniczne jest relatywnie łatwy, o tyle w przypadku pracy zdalnej może być – i jak pokazuje praktyka często jest – znacznie utrudniony.

Podstawowym narzędziem wykorzystywanym do komunikacji jest poczta elektroniczna. Może być ona źródłem potencjalnych zagrożeń związanych z wyciekiem danych. Ataki phishingowe, hakerskie, próby wyłudzenia danych czy inne niebezpieczne zjawiska w kontekście pracy zdalnej mogą intensyfikować się wraz z upowszechnianiem się tej formy zatrudnienia. Dzieje się tak dlatego, że pracownik pracujący w określonej odległości od biura staje się potencjalnie łatwym celem.

Pracodawcy powinni w tym kontekście zadbać, by ich pracownicy odbyli odpowiednie szkolenia w tym zakresie. Podstawą jest korzystanie ze służbowych skrzynek mailowych wygenerowanych przez specjalistów w środowisku świadczenia pracy. Absolutnie

niedopuszczalne powinno być – co jednak wciąż ma miejsce – korzystanie z prywatnych kont e-mail. Pracownicy powinni zdobyć wiedzę, która pozwoli im rozpoznać zagrożenia i przeciwdziałać im. Mowa tu o szeregu absolutnie fundamentalnych zasad takich jak choćby zakaz otwierania wiadomości wysłanych z nieznanych lub podejrzanych adresów czy domen, zakaz pobierania załączników lub pobieraniem plików, które takie wiadomości zawierają czy wczytywanie linków niewiadomego pochodzenia. Przestrzeganie tych zasad może uchronić nas przed pobraniem choćby niebezpiecznego oprogramowania, które może doprowadzić do wycieku np. danych wrażliwych. Korzystanie z prywatnych skrzynek e-mail wiąże się także ze zwykle niższym poziomem zabezpieczeń, którymi dysponujemy w środowisku sieci domowej.

W wielu przypadkach – zarówno przy korzystaniu ze skrzynek e-mail jak i na przykład używania środowiska chmurowego – sprawdzoną metodą jest zamieszczanie możliwie najczęściej plików zaszyfrowanych. Należy przy tym pamiętać, że hasło nie powinno być przesłane tym samym kanałem, którym wysłany został plik.

W przypadku korzystania z rozwiązań chmurowych to na administratorze spoczywa obowiązek analizy i zapewnienia odpowiedniego poziomu bezpieczeństwa danych. Dlatego właśnie tak istotne jest, aby przed podjęciem decyzji o digitalizacji upewnić się, że wybrane przez nas narzędzie posiada odpowiedni poziom zabezpieczeń, który w sytuacji kryzysowej mógłby zapobiec wyciekowi danych czy ich utracie.

Bezpieczeństwo danych, a właściwy wybór urządzenia

Podobnie jak ma to miejsce w przypadku skrzynek poczty elektronicznej, także korzystanie z urządzeń takich jak komputery, tablety czy telefony powinno odbywać wyłącznie przy użyciu sprzętu służbowego. Administrator powinien upewnić się, że urządzenia te zabezpieczone są silnymi hasłami lub uwierzytelnianiem wieloskładnikowym. Podjęcie decyzji o formule zdalnej jako o metodzie świadczenia pracy może być okazją do przeglądu zabezpieczeń i weryfikacji ich funkcjonalności.

Sprzęt służbowy powinien być zaopatrzony w możliwie najbardziej aktualne oprogramowanie, systemy tworzenia zapasowych kopii danych w czasie rzeczywistym czy zaktualizowany program antywirusowy. Sprzęt przeznaczony do pracy nie powinien być także wykorzystywany do spraw prywatnych. Eksperci postulują także, aby pracownicy, po zakończeniu korzystania ze sprzętu służbowego, stosowali zasadę tak zwanego czystego biurka, polegającą na zablokowaniu dostępu do urządzenia po opuszczeniu swojego stanowiska. Podobne zasady dotyczą korzystania ze smartfonów, które – dzięki postępowi technologicznemu – z powodzeniem służyć mogą jako alternatywa dla standardowego sprzętu komputerowego. Pamiętać należy także, aby w przypadku korzystania z urządzeń służbowych, korzystać wyłącznie z zaufanych sieci. Dobrą metodą jest w tym przypadku także wdrożenie protokołu VPN. To szczególnie istotne w kontekście prób łączenia się z sieciami publicznymi. Eksperci radzą także, aby – mając wybór pomiędzy siecią publiczną, a możliwością udostępnienia internetu na przykład ze służbowego smartfona – skorzystać bezsprzecznie z drugiej opcji.

Bezpieczne zarządzanie dokumentacją papierową w kontekście pracy zdalnej

Eksperci z zakresu ochrony danych podkreślają, że potencjalnie niebezpiecznym działaniem może być niewłaściwe korzystanie z dokumentacji papierowej. O ile jest to możliwe, w kontekście pracy zdalnej zaniechać powinno się drukowania dokumentów. Dobrą praktyką jest także wykorzystywanie niszczarki lub przechowywanie dokumentacji w miejscach bezpiecznych. Także skanowanie powinno być odbywać się w sposób maksymalnie ograniczający możliwość wycieku informacji. Zaleca się, aby nie gromadzić w ten sposób zdigitalizowanych dokumentów w pamięci urządzeń przenośnych, a wyłącznie we wskazanym przez administratora środowisku chmurowym lub w pamięci zabezpieczonych dysków.

Podsumowanie

Pracodawcy, decydując się na pracę zdalną, powinni stworzyć pakiet dokumentów, które zawierać będą konieczne regulacje dotyczące organizacji pracy w formule zdalnej. Regulaminy określać powinny nie tylko zasady bezpieczeństwa opisane powyżej, ale także czas pracy,

zasady raportowania, wskazane i zabronione metody komunikacji czy przesyłania i gromadzenia danych.

Kwestia ta dotyczy w szczególności branż, w których praca zdalna odgrywa i odgrywać będzie największą rolę, a więc w sektorze IT oraz e-commerce. Nie znaczy to jednak, że inne instytucje, przedsiębiorstwa czy organizacje zaniechać mają wdrażania procedur związanych z ochroną i bezpieczeństwem danych. Potrzeby w tym zakresie były, są i pozostaną znaczące. Gdy pod uwagę weźmiemy wyniki badania *Oczekiwania, potrzeby i postawy pracowników dotyczące pracy zdalnej* zrealizowanego na zlecenie Związku Przedsiębiorców i Pracodawców w ramach projektu *Potrzeby i wyzwania związane z wdrożeniem w przedsiębiorstwach prywatnych modelu pracy zdalnej*, zauważymy, że jeden na dziesięciu pracowników wykonuje swoje obowiązki właśnie w formule zdalnej, a aż ¾ wyraża opinię, że praca zdalna jest rozwiązaniem wskazanym nie tylko w sytuacjach kryzysowych. Może to wieszczyć pewną zmianę względem okresu sprzed pandemii – efektem może być zauważalne przesunięcie formuły świadczenia pracy w kierunku pracy zdalnej. Wciąż także, jak wskazuje badanie ZPP, podnoszone są argumenty przemawiające za wdrażaniem zdalnej formuły świadczenia obowiązku pracy. 57 procent badanych wskazuje tu na oszczędność czasu, a 39 procent na oszczędność środków finansowych. Praca zdalna zwiększa też możliwości rekrutacyjne którymi dysponują pracodawcy, na co – jako niewątpliwą zaletę – wskazuje 54 procent respondentów. Znikają wówczas choćby bariery regionalne – także w kontekście zatrudniania pracowników spoza granic Polski. Aż 65 procent pytanych wskazało tu, że praca w formule zdalnej to także redukcja kosztów zatrudnienia dla pracodawcy.

Należy spodziewać się, że praca zdalna stawać się będzie – w myśl trendu globalizowania się procesów biznesowych – coraz bardziej obecna także na polskim rynku pracy. Stąd ustawowe sformalizowanie jej charakteru, nawet wyraźnie spóźnione, odczytane zostało przez środowiska pracowników i pracodawców jako działanie pożądane.