RODO

Ochrona danych osobowych na prywatnym sprzęcie pracownika: 5 pytań po karze prezesa UODO

Dane osobowe wykorzystywane przez pracownika powinny być przetwarzane zgodnie z przepisami rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (dalej: RODO) nie tylko na służbowym, lecz także na prywatnym sprzęcie, na którym wykonuje on swoje obowiązki. Takie stanowisko wyraził Wojewódzki Sąd Administracyjny w wyroku z 5 października 2023 r., podtrzymując karę upomnienia nałożoną przez prezesa Urzędu Ochrony Danych Osobowych (UODO) na rzecznika finansowego.
Podstawą do nałożenia kary był brak przeprowadzenia przez rzecznika jako administratora danych analizy ryzyka w związku z pracą zdalną i korzystaniem przez pracowników z prywatnych i służbowych komputerów. Zdaniem organów wykazałaby ona potrzebę wprowadzenia odpowiednich rozwiązań m.in. na wypadek kradzieży prywatnego komputera, do czego doszło w analizowanej sprawie.
Od kiedy powszechnie stosujemy pracę zdalną, zagadnienie to stało się bardzo istotne dla wielu pracodawców. Poniżej przedstawiam najczęstsze wątpliwości pracodawców, z jakimi można się spotkać na tle przytoczonej sprawy w kontekście bezpiecznego umożliwienia pracownikom wykorzystywania ich prywatnego sprzętu do pracy na służbowych danych.

Agata Majewska
radca prawny,
Ślązak Zapiór i Partnerzy

1. Czy pracodawca odpowiada za dane osobowe, jakie pracownik przetwarza, wykonując pracę na swoim prywatnym sprzęcie?

Powszechnie wydaje się, że pracodawca jako administrator danych osobowych odpowiada za ich zgodne z prawem przetwarzanie wyłącznie wtedy, gdy dzieje się to w należącej do niego infrastrukturze. Tymczasem przepisy nie przewidują takiego ograniczenia. Wręcz przeciwnie – RODO wskazuje, że to pracodawca jako administrator ustala cele i sposoby przetwarzania danych osobowych, a więc także to, przy pomocy jakich narzędzi i w jakich obszarach ono się odbywa. Stosownie do tych okoliczności powinien on również dokonać analizy ryzyka dla bezpieczeństwa przetwarzanych danych i wdrożyć adekwatne do tych ryzyk środki bezpieczeństwa.

Zaznaczył to również WSA we wspomnianym wyżej wyroku, gdzie podkreślił, że ochrona danych osobowych, jakie pracownik przetwarza na swoim prywatnym komputerze w celach związanych z pracą, jest obowiązkiem pracodawcy jako administratora tych danych. Nie zmienia tego nawet ustanie zatrudnienia danej osoby. Dlatego tak ważna jest bieżąca weryfikacja tego, jakie sposoby przetwarzania w organizacji dopuszcza administrator, w tym, czy przewiduje możliwość pracy na prywatnym sprzęcie pracowników, a jeśli tak – jakie standardy bezpieczeństwa nakłada na nich w tym zakresie.

WSA podkreślił również, że pracownik nie występuje jako odrębny podmiot prawa, a jego działania są de facto działaniami pracodawcy, za które ten ostatni ponosi odpowiedzialność. Pamiętać musimy, że zgodnie z art. 29 RODO to na pracodawcy spoczywa obowiązek dopilnowania, by każda osoba działająca z jego upoważnienia i mająca dostęp do danych osobowych przetwarzała je wyłącznie na jego polecenie jako administratora.

To pracodawca decyduje więc o tym, w jaki sposób dane przetwarzane przez upoważnione przez niego osoby powinny być wykorzystywane – w tym również przy użyciu jakiego sprzętu. Dodatkowo aspekty te powinien pracodawca jako administrator danych osobowych uwzględnić w prowadzonej analizie ryzyka, która towarzyszyć powinna każdemu procesowi przetwarzania.

2. Czy wykorzystywanie prywatnego sprzętu przez pracownika nie powoduje, że to on jest wyłącznie odpowiedzialny za dane, jakie w nim przechowuje?

Musimy pamiętać, że zarówno na płaszczyźnie pracowniczej, jak i ochrony danych osobowych pracownik, wykonując swoje obowiązki, działa w granicach polecenia i upoważnienia pracodawcy występującego co do zasady w roli administratora danych osobowych. Działa on więc w imieniu pracodawcy.

To pracodawca zaś decyduje o tym, jakie sposoby przetwarzania danych osobowych i ich zabezpieczenia dopuszcza. Jeśli pozwala na przetwarzanie przez pracownika zadań na jego prywatnym sprzęcie, powinien uwzględnić to jako dodatkowy czynnik ryzyka. Wykorzystywanie do pracy np. domowego komputera wiąże się bowiem przede wszystkim z reguły z niższym poziomem zabezpieczeń informatycznych, korzystaniem z tego sprzętu przez członków rodziny pracownika, ze zwiększonym ryzykiem kradzieży itp.

Pracodawca powinien dokonać kompleksowej analizy ryzyka dla ochrony danych na potrzeby procesu pracy zdalnej, która uwzględniać musi posiadane zasoby, zakres przetwarzanych danych, stosowane środki bezpieczeństwa oraz wynikający z tych okoliczności poziom ryzyka naruszenia ich poufności, dostępności i integralności. Dopiero jeśli uzna, że poziom tego ryzyka jest dla niego akceptowalny, może dopuścić możliwość pracy zdalnej przy użyciu prywatnego sprzętu, odpowiednio zabezpieczając stosowanie przez zatrudnionych przyjętych standardów bezpieczeństwa. Odpowiedzialność za bezpieczeństwo przetwarzanych danych osobowych w pierwszej kolejności ponosi bowiem właśnie administrator. Dotyczy to zarówno odpowiedzialności administracyjnej przed prezesem Urzędu Ochrony Danych Osobowych, jak i odszkodowawczej – wobec samego podmiotu danych.

Dopiero w razie zawinionego naruszenia przez pracownika przyjętych w organizacji zasad bezpieczeństwa pracodawca może egzekwować jego odpowiedzialność. O ile osoba taka pozostaje jeszcze w zatrudnieniu, można mówić tu o odpowiedzialności porządkowej, materialnej lub rozwiązaniu umowy o pracę. Jeśli naruszenia dopuścił się były pracownik, to w grę wchodzi wyłącznie odpowiedzialność odszkodowawcza na zasadach określonych w kodeksie cywilnym.

O odpowiedzialności pracownika mówić można jedynie w sytuacji, w której nie zastosował się on do poleceń i standardów bezpieczeństwa określonych jasno przez pracodawcę. Brak będzie dla niej podstaw, jeśli pracodawca nie dopilnował tego, by pracownik w odpowiedni sposób zabezpieczył dane przetwarzane na własnym sprzęcie. Zarówno w decyzji prezesa UODO, jak i w wyroku WSA w przypomnianej wyżej sprawie podkreślono, że pracodawca nie tylko nie zobowiązał pracownika do szyfrowania dysku twardego na jego komputerze, lecz także nie zweryfikował, czy skutecznie usunął on dane ze swojego komputera w związku z rozwiązaniem jego umowy o pracę.

3. Czy pracownik ma obowiązek zgłosić kradzież swojego prywatnego komputera lub telefonu?

Należy jeszcze raz zaznaczyć, że to administrator danych osobowych stoi na pierwszym froncie w kwestii zapewnienia bezpieczeństwa danych osobowych w organizacji. To on przede wszystkim ponosi odpowiedzialność za jego naruszenie. Również to on ma obowiązek dokonać zgłoszenia naruszenia do prezesa UODO, jeśli uzna, że dane zdarzenie pociąga za sobą realne ryzyko naruszenia praw lub wolności podmiotu danych. By zrealizować te obowiązki, musi mieć wiedzę o wszelkich okolicznościach wpływających na poziom bezpieczeństwa administrowanych przez siebie danych. Dlatego też utrata przez pracownika nośnika, na którym przetwarza dane w imieniu pracodawcy, powinna zostać zgłoszona mu niezwłocznie – niezależnie od tego, czy jest to powierzony mu firmowy nośnik, czy jego prywatny sprzęt, w tym komputer osobisty. Decydującego znaczenia nie ma bowiem to, czyją własność stanowi nośnik danych, ale który podmiot jest odpowiedzialny za zapewnienie odpowiedniego poziomu bezpieczeństwa zgromadzonych na nim danych jako ich administrator (względnie podmiot przetwarzający).

Pracownicy muszą wiedzieć, że ich obowiązkiem jest niezwłoczne zgłoszenie pracodawcy kradzieży, utraty lub zaatakowania przez złośliwe oprogramowanie również własnego sprzętu, jeśli tyko przetwarzają na nim dane służbowe. Taki obowiązek trzeba wprost sformułować w wewnętrznych dokumentach, takich jak polityka bezpieczeństwa informacji lub ochrony danych, regulamin pracy zdalnej, indywidualna umowa z pracownikiem itp.

4. Jak odpowiednio zabezpieczyć dane przechowywane przez pracownika na prywatnym sprzęcie?

Ważne, by w tym zakresie działać profilaktycznie i zapobiegawczo, a nie jedynie następczo. Jak pokazuje omawiana sprawa, kluczowe jest odpowiednie zaprojektowanie procesu przetwarzania danych przy użyciu prywatnego sprzętu pracowników, także poza obszarem i infrastrukturą przestrzenną lub informatyczną pracodawcy.

Służyć temu powinna przede wszystkim analiza ryzyka tego procesu dla ochrony danych. Co ważne, powinna ona mieć charakter ciągły i uwzględniać wszystkie pojawiające się nowe czynniki, jak właśnie fakt wykorzystywania własnego sprzętu, wykonywanie pracy zdalnej za granicą, nowe rozwiązania informatyczne, nowe rodzaje zagrożeń cybernetycznych itp.

Współgrać z bieżącą analizą powinien odpowiedni system zabezpieczeń przetwarzanych danych, zarówno tych organizacyjnych, jak i technicznych, informatycznych. Istotne jest też odpowiednie, jednoznaczne i zrozumiałe dla pracowników uregulowanie zasad korzystania z własnego sprzętu na poziomie organizacji. Odpowiednie postanowienia w tym zakresie powinny znajdować się w przywołanej już wcześniej polityce bezpieczeństwa, regulaminie pracy zdalnej itp.

Kluczowa jest tu świadomość pracowników, zarówno pod kątem zagrożeń wiążących się z pracą w środowisku informatycznym, jak i tych związanych z pracą zdalną wykonywaną najczęściej w warunkach domowych.

5. Czy pracodawca może wyciągnąć konsekwencje od pracownika, który nieodpowiednio zabezpieczy na własnym komputerze dane osobowe przetwarzane w związku z pracą?

Zgodnie z przepisami kodeksu pracy określającymi zasady pracy zdalnej wewnętrzny regulamin lub porozumienie z pracownikiem powinny ustalać zasady kontroli przestrzegania wymogów w zakresie bezpieczeństwa i ochrony informacji, w tym procedur ochrony danych osobowych. Ważne jednak, by zasady te były dla pracowników jasne i zrozumiałe, by mogli się do nich stosować.

Pracodawca ma również obowiązek określić procedury ochrony danych osobowych i przeprowadzić, w miarę potrzeby, instruktaż i szkolenie na potrzeby wykonywania pracy zdalnej – niezależnie od tego, czy dopuszcza używanie przez pracownika jego własnego sprzętu, czy nie. Jeśli jednak przewiduje taką możliwość, to procedura, instruktaż i szkolenie powinny uwzględniać tę okoliczność i wynikające stąd dodatkowe ryzyka.

Dla skutecznego dochodzenia potencjalnej odpowiedzialności od pracownika za naruszenie zasad bezpieczeństwa ochrony danych przy pracy zdalnej powinien on potwierdzić (na piśmie lub elektronicznie), że zapoznał się z firmowymi procedurami oraz jest świadomy swojego obowiązku ich przestrzegania.

Wyrażając zgodę na pracę na własnym sprzęcie pracownika, pracodawca w razie potencjalnego incydentu ochrony danych nie może pociągnąć go do odpowiedzialności z powodu niezastosowania metod zabezpieczenia danych, do których uprzednio wyraźnie go nie zobowiązał.

Wątpliwa może być również skuteczność zobowiązania pracownika do zastosowania metod zabezpieczeń, których obiektywnie nie jest w stanie zapewnić, chociażby z uwagi na brak ich dostępności dla oprogramowania w wersji osobistej lub wysoki koszt dostępnych na rynku zabezpieczeń. W takim wypadku pracodawca powinien rozważyć, czy okoliczności te nie oznaczają braku możliwości wykorzystywania własnych narzędzi do pracy zdalnej bądź też konieczności zapewnienia pracownikowi środków na sfinansowanie zabezpieczeń.

Zwracał na to uwagę również WSA, który zaznaczył, że pracodawca powinien być w stanie wykazać, że prywatny komputer pracownika został odpowiednio zabezpieczony przed potencjalnym nieuprawnionym dostępem do zgromadzonych na nim danych osobowych. Ważne jest, aby pracownik łączył się przez VPN, korzystał z odpowiednich programów do szyfrowania plików oraz stosował hasła do logowania.

Wszystkie wymienione wyżej okoliczności są o tyle istotne, gdyż dopiero wówczas zawinione naruszenie obowiązków przez pracownika pozwala pracodawcy na skuteczne pociągnięcie go odpowiedzialności porządkowej lub materialnej, a nawet na rozwiązanie umowy o pracę. ©℗

Podstawa prawna

- art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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) (Dz.Urz. UE z 2016 r. L 119, s. 1)
- ustawa z 23 kwietnia 1964 r. – Kodeks cywilny (t.j. Dz.U. z 2023 r. poz. 1610; ost.zm. Dz.U. z 2023 r. poz. 1933)
- ustawa z 26 czerwca 1974 r. – Kodeks pracy (t.j. Dz.U. z 2023 r. poz. 1465)