Dziennik Gazeta Prawna B
19.11.19 nr: 223 str. 1 nakład: 47000 egz.

Uczelni grozi pozew za kradzież laptopa jednego z jej pracowników

RODO Tysiące osób rozważa wytoczenie sprawy Szkole Głównej Gospodarstwa Wiejskiego w Warszawie w związku **z potencjalnym wyciekiem ich danych**

Sławomir Wikariak
slawomir.wikariak@infor.pl

Informację o kradzieży laptopa, na którym przechowywano szczegółowe dane kandydatów na studia, SGGW opublikowała w czwartek. Już następnego dnia na Facebooku została założona grupa „Pozew zbiorowy w sprawie RODO SGGW". Wczoraj liczyła ona już prawie 14 tys. członków. Szybko zorientowali się oni, że pozew zbiorowy nie wchodzi w grę, bo w postępowaniu grupowym nie można dochodzić zadośćuczynienia. Nie zrezygnowali jednak z roszczeń.

Autorzy specjalnie założonej strony internetowej www.pokrzywdzenisggw.pl zachęcają do zgłaszania się osoby, których dane mogły wyciec. Nawiązali już współpracę z kancelarią prawną, która ma im pomóc w pozwaniu uczelni. Jednocześnie zachęcają osoby potencjalnie poszkodowane, by składały skargi na SGGW do Urzędu Ochrony Danych Osobowych.

– Nasze zarzuty wobec SGGW są proste: nie wdrożono odpowiednich środków technicznych ani organizacyjnych pozwalających na przetwarzanie danych osobowych zgodnie z RODO, nie zapewniono bezpieczeństwa i zaniedbano realizację obowiązku przetwarzania danych wyłącznie przez osoby wskazane przez administratora – wylicza Kinga Rozmuszyńska, jedna z inicjatorek akcji.

Podkreśla, że w jej ocenie uczelnia nienależycie informowała o potencjalnym wycieku. Komunikat o zagrożeniu umieściła na swej stronie internetowej dopiero 14 listopada, a laptop z danymi kandydatów został skradziony już 5 listopada.

Aby sąd uznał roszczenie, poszkodowany musi wykazać szkodę. Nie musi być ona jednak majątkowa

Domniemanie winy

Poproszeni przez nas o komentarz prawnicy nie wykluczają, że roszczenia finansowe kandydatów na studia mogą być uzasadnione.

Maciej Gawroński, partner zarządzający w kancelarii Gawroński & Partners, wyjaśnia, że bezpośrednią podstawą takich roszczeń jest art. 82 RODO, który pozwala pozywać o wszelkiego typu szkody, a także o zadośćuczynienie (czyli w tym przypadku może to być odszkodowanie choćby za strach).

– Oznacza to, że nawet jeśli jeszcze nie doszło do wykorzystania naszych danych, możemy dochodzić: zadośćuczynienia za narażenie nas na obawę przed kradzieżą tożsamości i koszty poniesione w celu ograniczenia ryzyka negatywnych konsekwencji (np. koszty wymiany dowodu osobistego, zastrzeżenia numeru PESEL w bazach firm pożyczkowych). W USA tego typu roszczenia są na razie ryczałtowane na poziomie kilkuset dolarów. Jednak jest to wczesny etap ucierania się praktyki – zauważa ekspert.

Osoby, które czują się poszkodowane, nie muszą więc uzależniać kroków prawnych od tego, czy ich dane rzeczywiście zostaną wykorzystane np. do wzięcia kredytu. Jeśli złodziejowi zależało wyłącznie na wartości samego komputera, to być może dane są bezpieczne i nigdy nie zostaną użyte.

Jednak nawet i bez tego SGGW musi się liczyć z możliwością poniesienia odpowiedzialności. Artykuł 82 ust. 3 RODO zwalnia z niej tylko wówczas, gdy administrator danych w żaden sposób nie ponosi winy za zdarzenie. Tu zaś byłoby to trudne – można mówić chociażby o winie w nadzorze nad pracownikiem, który niefrasobliwie skopiował dane na dysk przenośnego komputera. Zgodnie ze słowami Krzysztofa Szwejka, rzecznika prasowego uczelni, pracownik złamał w ten sposób obowiązujące procedury.

Musi być szkoda

Żeby jednak takie roszczenie zostało uznane przez sąd, należy wykazać szkodę.

– W tym przypadku może być ona majątkowa, gdyby faktycznie doszło do uzyskania kredytów na dane osobowe studentów, albo niemajątkowa, a więc opierająca się na zasadzie krzywdy, np. na cierpieniu psychicznym spowodowanym nieuprawnionym dostępem do danych osobowych – komentuje Piotr Liwszic, specjalista ds. ochrony danych w ODO 24.

Dodaje, że konieczne będzie wykazanie związku między powstałą szkodą a działaniem do niej doprowadzającym oraz udowodnienie winy.

– W przypadku dochodzenia odszkodowania lub zadośćuczynienia na podstawie przepisów RODO mamy do czynienia z domniemaniem winy administratora danych, a więc uczelni – dodaje ekspert.

Wielu zagrożonych

Osoby, których dane mogły wyciec, nie kryją frustracji.

– Musimy podjąć działania, żeby chronić się przed skutkami tego wycieku. Co gorsza, w Polsce nie ma możliwości zmiany numeru PESEL, a banki i pożyczkodawcy nie mają obowiązku sprawdzania, czy ktoś nie zastrzegł dokumentów – wylicza Kinga Rozmuszyńska.

Jedną z głównych obaw pokrzywdzonych jest właśnie wykorzystanie ich danych do zaciągnięcia kredytu.

Nie wiadomo dokładnie, ile osób może mieć problem w związku z potencjalnym wyciekiem.

„Nie wiemy, z ilu lat pracownik przechowywał dane na komputerze. To właśnie wyjaśniają policja i prokuratura. Toczy się śledztwo w tej sprawie. (...) Prawdopodobnie komputer skradziono przypadkowo, ale ponieważ nie wiemy, ile rekordów bezprawnie było zapisanych na tym komputerze i czy dojdzie do ich wykorzystania, postanowiliśmy opublikować komunikat i personalnie powiadomić wszystkie osoby, które do nas aplikowały w ostatniej rekrutacji" – napisał w komunikacie Krzysztof Szwejk.

Klucz w szyfrowaniu

Wiele osób uważa, że te dane w ogóle nie powinny być przekopiowane na laptopa. Z komunikatu uczelni wynika, że ona również uważa to za złamanie wewnętrznych procedur.

W rzeczywistości jednak nie to jest najważniejsze w tej sprawie. Kluczowe jest to, jak były zabezpieczone te informacje.

Doktor Łukasz Olejnik, niezależny badacz i doradca cyberbezpieczeństwa i prywatności, związany z Center for Technology and Global Affairs Uniwersytetu Oksfordzkiego, wskazuje, że dane znajdujące się na laptopach to rzeczywistość, z którą można się spotkać w wielu organizacjach.

– Warto się jednak zastanowić, czy wynoszenie takich danych w znacznych ilościach poza siedzibę organizacji jest w ogóle konieczne. Jeśli tak, to wrażliwe dane muszą się znajdować na sprzęcie odpowiednio zabezpieczonym, pod kontrolą – tłumaczy ekspert.

Wyjaśnia, że dziś istnieją dojrzałe rozwiązania szyfrujące cały dysk.

– To może być choćby FileVault lub BitLocker, których działanie i oferowane zalety są dobrze zrozumiałe. W połączeniu z dobrym hasłem to minimalna obowiązkowa podstawa. Choć niekoniecznie jest wystarczająca, ale zapewnia ochronę przed typowym ryzykiem fizycznej utraty sprzętu w wyniku kradzieży – dodaje Łukasz Olejnik.

Czy ten laptop był zabezpieczony, a jeśli tak, to w jaki sposób? Rzecznik SGGW nie odpowiedział na przesłane mu wczoraj pytania.

UODO analizuje

Urząd Ochrony Danych Osobowych na razie nie otrzymał żadnych skarg od poszkodowanych. Sam incydent został mu natomiast zgłoszony przez SGGW. Trwa analiza tego zgłoszenia, a ewentualne dalsze działania UODO będą uzależnione od ujawnionych okoliczności.

– Moim zdaniem warto poczekać na działania prezesa UODO, a szczególnie na prawomocną decyzję dotyczącą stwierdzenia naruszenia przepisów RODO. Takie ustalenie wiąże sąd w postępowaniu o naprawienie szkody wyrządzonej przez naruszenie przepisów o ochronie danych osobowych właśnie w zakresie stwierdzenia takiego naruszenia – zwraca uwagę Piotr Liwszic.

Dodaje, że jeżeli ktoś chce skorzystać ze ścieżki sądowej, powinien pamiętać, że sąd jest zobligowany do zawieszenia postępowania cywilnego w związku z prowadzeniem przez prezesa UODO sprawy. ©℗

BARDZO SZCZEGÓŁOWE DANE

Na skradzionym komputerze znajdowały się dane kandydatów na studia, w tym:

- imię,
- drugie imię,
- nazwisko,
- nazwisko rodowe,
- imiona rodziców,
- PESEL,
- płeć,
- narodowość,
- obywatelstwo,
- adres zamieszkania,
- seria i numer dowodu/paszportu,
- seria i numer dowodu osobistego,
- ukończona szkoła średnia,
- miejscowość szkoły średniej,
- numer telefonu komórkowego i stacjonarnego,
- rok ukończenia szkoły średniej,
- numer i data świadectwa ukończenia szkoły średniej,
- rok matury i data świadectwa maturalnego,
- wyniki uzyskane na egzaminie maturalnym,
- ukończone studia,
- informacja o zakwalifikowaniu na studia oraz punkty kwalifikacyjne kandydata.

5364
SKARGI
WPŁYNĘŁY DO UODO OD POCZĄTKU ROKU DO KOŃCA SIERPNIA 2019 R.

3610
ZGŁOSZEŃ
O NARUSZENIU OCHRONY DANYCH (W TYM O WYCIEKACH) ZGŁOSILI ADMINISTRATORZY DO UODO W CIĄGU PIERWSZYCH OŚMIU MIESIĘCY 2019 R.

©℗ RM