

WYWIAD \ Z ANDRZEJEM LEWIŃSKIM, zastępcą Generalnego Inspektora Ochrony Danych Osobowych (GIODO), rozmawia PIOTR NISZTOR

Jak się bronić przed kradzieżą tożsamości

Kradzieże tożsamości to dziś bardzo poważny problem, tym bardziej groźny, że często zaciągając kredyt przez internet, nie zastanawiamy się np., czy oferujące je firmy korzystają z bezpiecznych połączeń – mówi w wywiadzie dla „Gazety Polskiej Codziennie” ANDRZEJ LEWIŃSKI.

Zmiany dotyczące ochrony danych będą obowiązywały dopiero za dwa lata, w połowie 2018 r. Dlaczego więc już teraz przedsiębiorstwa i wszystkie instytucje przetwarzające dane osobowe powinny się do tego przygotowywać?

Niedawno podczas wykładu w SGH z bezpieczeństwa informatycznego zapytałem słuchaczy, ilu wśród nich jest administratorów bezpieczeństwa informacji (ABI) odpowiadających za ochronę danych osobowych. Rękę podniosła tylko jedna osoba – był to informatyk. Na zakończenie spotkania poprosiłem go, żeby powiedział, co myśli o przygotowaniu instytucji i firm do stosowania przepisów unijnego rozporządzenia o ochronie danych osobowych, które zacznie bezpośrednio obowiązywać od 25 maja 2018 r. Powiedział krótko – to będzie masakra. Żeby tak się nie stało, przygotowania do mających nastąpić zmian należy rozpocząć już teraz, bo to skomplikowany proces, którego nie uda się przeprowadzić w ciągu kilku miesięcy.

Trzeba pamiętać, że rozporządzenie wprowadza zupełnie nowe spojrzenie na pozycję administratora danych i to na niego przenosi ciężar odpowiedzialności za przetwarzanie danych osobowych niezgodnie z prawem. Konsekwencją tego są wysokie kary finansowe, które GIODO będzie mógł nakładać za naruszenia związane z ochroną danych osobowych. Ich górna granica to 20 mln euro, a w wypadku przedsiębiorstw – 4 proc. rocznego światowego obrotu z poprzedniego roku obrotowego. Jak widać to naprawdę dużo, choć te najwyższe kary będą stosowane przy rażącym naruszeniu przepisów, skutkującym dużą szkodą dla osoby, której dane są przetwarzane. Wśród niektórych państw członkowskich UE podobne przepisy funkcjonują już od dawna, ale w Polsce to będzie nowość.



Andrzej Lewiński | fot. Zbyszek Kaczmarek/Gazeta Polska

Obecnie funkcjonujące przepisy też dają GIODO możliwość nakładania kar finansowych. Ile razy skorzystano z tego uprawnienia w ostatnich latach?

Obecnie GIODO nie ma uprawnień do nakładania kar pieniężnych za niezgodne z prawem przetwarzanie danych osobowych. GIODO – jako organ egzekucyjny w zakresie egzekucji administracyjnej obowiązków o charakterze niepieniężnym – może jedynie zastosować środek egzekucyjny w postaci nałożenia na zobowiązanego grzywny w celu przymuszenia do wykonania wydanej przez niego decyzji. Dotychczas stało się tak w dwóch wypadkach, w których GIODO, korzystając ze swoich ustawowych uprawnień, nałożył cztery grzywny na łączną kwotę 130 tys. zł (dwie grzywny po 25 tys. zł i dwie po 40 tys. zł). Obydwa podmioty wykonały nakazy decyzji GIODO, grzywny w wysokości 25 tys. zł zostały wyegzekwowane przez GIODO, natomiast grzywny w wysokości 40 tys. zł w związku z wykonaniem decyzji zostały umorzone. Przepisy, na podstawie których GIODO zyskał takie uprawnienia, obowiązują od 7 marca 2011 r.

Obowiązujące przepisy za naruszenia związane z ochroną danych osobowych przewidują odpowiedzialność karną. Dlaczego w praktyce to fikcja?

Liczba naruszeń dotyczących niezarejestrowania zbiorów danych osobowych, niewykonania obowiązku informacyjnego, wpływu danych czy ich przetwarzania bez podstawy prawnej jest bardzo duża. Myślę, że GIODO mógłby dziennie wysyłać do prokuratur około kilkudziesięciu zawiadomień o podejrzeniu popełnienia przestępstwa. Najczęściej jednak nakazuje przywrócenie stanu zgodnego z prawem, a zawiadomienia wysyła w wypadku najbardziej rażących naruszeń. Niestety, większość takich spraw jest umarzana z powodu niskiej szkodliwości społecznej czynu, na co zwracaliśmy uwagę w korespondencji kierowanej do Prokuratora Generalnego. Na szczęście także w organach ścigania rośnie świadomość w tym zakresie i zrozumienie sytuacji. Mam nadzieję, że przyczyni się to do zmiany istniejącego do niedawna wśród administratorów danych poczucia bezkarności za nieprzestrzeganie obowiązujących ich przepisów prawa.

Teraz wójt, prezydent czy prezes spółki handlowej wiedzą, że pociągnięcie ich do odpowiedzialności karnej za naruszenia związane z ochroną danych osobowych może dla nich oznaczać zakaz sprawowania funkcji.

A za dwa lata, gdy zacznie obowiązywać unijne rozporządzenie o ochronie danych osobowych, muszą liczyć się z karą 20 mln euro...

Kara może wynieść do 20 mln euro w wypadku bardzo poważnych naruszeń, do których zaliczyć można wyciek danych. Proszę jednak zauważyć, że w Polsce nie dochodzi do nich często i na tak dużą skalę, jak w innych krajach. Ostatnio grupa hakerów opublikowała w sieci bazę zawierającą dane osobowe 50 mln obywateli Turcji, w Stanach Zjednoczonych zaś z Głównego Urzędu Kadr Administracyjnych wyciekły informacje o 20 mln Amerykanów, w tym dane prezydenta i wiceprezydenta. Skuteczna ochrona danych osobowych więc to często kwestia bezpieczeństwa narodowego.

Jaką odpowiedzialność ponosi firma, w której dochodzi do wpływu

danych przez nieuwagę lub błąd któregoś z pracowników?

Obecnie, zgodnie z art. 51 ustawy o ochronie danych osobowych, za niezabezpieczenie danych osobowych odpowiedzialność karną ponosi nie tylko administrator danych, ale też każdy, kto był zobowiązany do ich zabezpieczenia. Niedawno w Krakowie pani z recepcji przychodni lekarskiej oddała do skupu makulatury historie chorób pacjentów. Wszczęto śledztwo z art. 276 kodeksu karnego, czyli w związku z przestępstwem m.in. niszczenia czy nieuprawnionej modyfikacji dokumentu. Grozi jej za to kara grzywny lub kara ograniczenia wolności albo pozbawienia wolności do lat dwóch.

Czy możemy spodziewać się sytuacji, w której GIODO stanie do walki z takimi koncernami, jak np. Facebook i będzie ścigał je za naruszenia przepisów o ochronie danych osobowych?

Tak, choć muszę też zaznaczyć, że już mamy sukces na tym polu. Posiłkując się orzecznictwem Trybunału Sprawiedliwości Unii Europejskiej, GIODO nakazał polskiemu oddziałowi Facebooka usunięcie danych osobowych, które zostały zamieszczone na profilu jednego z polskich użytkowników serwisu. Facebook stwierdził, że jako organ nie jesteśmy do tego uprawnieni, bo ich europejskie przedstawicielstwo znajduje się w Irlandii, zatem to tamtejszy odpowiednik GIODO miałby prawo rozpatrywać skargę. Tymczasem GIODO, powołując się na najnowsze orzeczenia TSUE i wskazując, że w Polsce mieści się spółka koncernu przetwarzająca dane osobowe, a Facebook kieruje swoją działalność do osób mieszkających na terytorium Polski, wywieślił, że jesteśmy uprawnieni do wydawania decyzji na podstawie polskich przepisów prawa. Korzystając z tego, nakazaliśmy usunięcie z serwisu kwestionowanych przez skarżącego treści.

Czyli każdy może żądać usunięcia informacji o sobie?

Tak, w uzasadnionych wypadkach ma do tego obecnie prawo, a unijne rozporządzenie stanowi o tym wprost, wskazując np. w motywie 65, że: „Każda osoba fizyczna powinna mieć prawo do sprostowania danych osobowych jej dotyczących oraz prawo do »bycia zapomnianym«, jeżeli zatrzymywanie takich danych narusza niniejsze rozporządzenie, prawo Unii lub prawo państwa członkowskiego, któremu podlega administrator”.