

Polacy nie dowiedzą się o tym, że ich dane wyciekły

PRYWATNOŚĆ Większość firm nie będzie musiała powiadamiać klientów o naruszeniu bezpieczeństwa ich danych osobowych. Informację taką przekażą nowemu urzędowi

Sławomir Wikariak
slawomir.wikariak@infor.pl

Gdy dwa i pół roku temu hacker włamał się do jednej z kancelarii prawnych i wykradł poufne dane jej klientów, Polacy dowiedzieli się o tym wyłącznie dlatego, że sam to ogłosił, żądając pół miliona euro za nieujawnienie plików. Sposób zachowania firm, w których doszło do wycieku danych, miał się zmienić wraz z nadejściem przepisów nowego unijnego rozporządzenia o ochronie danych osobowych 2016/679 (RODO). Okazuje się jednak, że w Polsce się nie zmieni. W najnowszej wersji projektu naszej krajowej ustawy o ochronie danych przewidziano bowiem zwolnienie z konieczności stosowania art. 34 RODO, czyli przepisu nakazującego informować zainteresowanych o naruszeniu bezpieczeństwa ich danych. Z wyłączenia tego będą mogły skorzystać firmy zatrudniające mniej niż 250 osób, które nie przetwarzają danych wrażliwych i nie przekazują danych innym firmom. Oznacza to większość polskich przedsiębiorców. Tylko najwięksi (np. banki, ubezpieczyciele czy serwisy takie jak Allegro czy Facebook) będą musieli informować o wycieku. Przeciętny sklep internetowy nie będzie już miał takiego obowiązku.

Podwójne standardy

Wyłączenie to nie podoba się nie tylko aktywistom walczącym o prawo do prywatności, ale także generalnemu inspektorowi ochrony danych osobowych. – Ludziom zwyczajnie należy się informacja o tym, że bezpieczeństwo ich danych zostało naruszone, co może stwarzać dla nich konkretne zagrożenia. Ich nieprzekazywanie ostatecznie uderzy w samych przedsiębior-

ców, gdyż zachwieje zaufaniem klientów – zauważa dr Edyta Bielak-Jomaa.

Ograniczanie obowiązków wynikających z RODO będzie powodować, że polskie regulacje będą odmienne od tych stosowanych w innych krajach UE.

– Trudno spotkać w Europie inny kraj z tak ekstremalnie dużym zakresem wyłączeń na obecnym etapie prac. Projekty brytyjskie, francuskie czy irlandzkie nakazują, aby obywatele otrzymywali informację o wyciekach danych. Danie im tej świadomości i szansy na podjęcie działań zapobiegawczych to przecież jeden z filarów RODO. Można powiedzieć, że między innymi po to ta regulacja została stworzona – analizuje dr Łukasz Olejnik, badacz i konsultant cyberbezpieczeństwa i prywatności.

– Jeśli powstaną podwójne standardy, to obywatele w Polsce będą widzieli, że traktuje się ich odmiennie niż na Zachodzie. Czy taki krok nie jest ryzykowny? Warto rozważyć wpływ na poziom zaufania do gospodarki, ale i jej konkurencyjność. Potrafię sobie wyobrazić konsumentów, którzy mając do wyboru dostawców usług wybiorą tych z krajów o wyższych standardach, gdzie firmy nie są skryte za takimi wyłączeniami – dodaje ekspert.

Informacja na stronie

Co ciekawe, art. 34 RODO, którego polskie firmy MŚP mają w ogóle nie stosować, nie jest wcale tak restrykcyjny, jak mogłoby się wydawać. Nie nakazuje on bowiem informować o wszystkich wyciekach, tylko o takich, które mogą powodować wysokie ryzyko naruszenia praw lub wolności osób.

– Jeśli intencją autorów projektu jest ograniczenie kosztów

związanych z informowaniem dużej liczby klientów, to RODO już to przewiduje. W przypadkach, gdy przekazanie takiej informacji wymagałoby niewspółmiernie dużego wysiłku, umożliwia bowiem np. wydanie publicznego komunikatu lub zastosowanie podobnego środka. Zatem korzystając z rozwiązań przewidzianych w RODO, można spełnić obowiązek przekazywania informacji o wycieku chociażby za pośrednictwem strony internetowej firmy. To nic nie kosztuje, a klienci mieliby szansę dowiedzieć się o zagrożeniu bezpieczeństwa ich danych, a w stosownych przypadkach otrzymać wskazówki czy rady, jak można zminimalizować ewentualne negatywne skutki naruszenia – podpowiada dr Edyta Bielak-Jomaa, GİODO.

Ministerstwo Cyfryzacji przyznaje, że rozważało różne możliwości.

– Można przykładowo po prostu ograniczyć zastosowanie art. 34 RODO w pewnych przypadkach bądź zmodyfikować formę realizacji wymogu notyfikacji. Projektodawca zdecydował się na pierwsze rozwiązanie, gdyż nie chciał powtarzać przepisów RODO. Norma, w świetle której wymóg notyfikacji miał następować w formie komunikatu dostępnego na stronie internetowej, stanowiłaby zasadniczo powtórzenie art. 34 ust. 3 lit. c RODO. A przepisy krajowe nie mogą powtarzać prawa unijnego – tłumaczy dr Maciej Kawecki, dyrektor departamentu zarządzania danymi MC.

Sygnal ostrzegawczy

Polskie przepisy nie będą natomiast wyłączały art. 33 RODO, w którym mowa o przekazaniu w ciągu trzech dni informacji o wycieku organowi stojącemu

O czym nie będą musiały informować polskie firmy

Art. 34 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 o ochronie danych osobowych

ZAWIADAMIANIE OSOBY, KTÓREJ DANE DOTYCZĄ, O NARUSZENIU OCHRONY DANYCH OSOBOWYCH

- ➔ Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
- ➔ Zawiadomienie, o którym mowa w ust. 1 niniejszego artykułu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b), c) i d).
- ➔ Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane w następujących przypadkach:
 - administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym dostęp do tych danych osobowych;
 - administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;
 - wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.
- ➔ Jeżeli administrator nie zawiadomił jeszcze osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, organ nadzorczy – biorąc pod uwagę prawdopodobieństwo, że to naruszenie ochrony danych osobowych spowoduje wysokie ryzyko – może od niego tego zażądać lub może stwierdzić, że spełniony został jeden z warunków, o których mowa w ust. 3.

na straży ochrony danych osobowych. W naszych warunkach będzie to Urząd Ochrony Danych Osobowych. Zdaniem resortu cyfryzacji zapewni to obywatelom poszanowanie ich praw.

– W przypadku wszczęcia postępowania z urzędu stronomi postępowania staną się: osoba, której dane zostały naruszone, i przedsiębiorca, który naruszenia się dopuścił – podkreśla dr Maciej Kawecki.

Nie wszyscy jednak uważają, że to wystarczy. Choćby dlatego, że liczy się czas. Zgodnie z art. 34 administrator powinien informować o wycieku „bez zbędnej zwłoki”, czyli w zasadzie niebawem po tym, jak sam go zidentyfikuje.

– Dzięki takiej informacji każdy może sam ocenić, na ile istotne są dla niego dane, które wyciekły, i jakie ryzyko może się wiązać z ich ujawnieniem. Jeśli jest to numer karty płatni-

czej, to być może uzna, że należy ją zablokować. Jeśli używa tego samego hasła w innych serwisach, to prawdopodobnie zechce je zmienić. Aby móc jednak podjąć takie kroki, musi wiedzieć, że do wycieku w ogóle doszło – tłumaczy Katarzyna Szymielewicz, prezeska Fundacji Panoptykon.

Jej zdaniem niepokojące jest to, że zwalnia się z obowiązku stosowania całego przepisu, zamiast poszukać alternatywnych form jego wykonania.

– Mogę się zgodzić, że wysyłanie do każdego klienta listu poleconego byłoby nadmiernie uciążliwe dla przedsiębiorcy. Dlaczego jednak rząd nie proponuje rozwiązań, które wiązałyby się z mniejszym nakładem środków, a jednocześnie realizowało istotę prawa, jaką w tym przypadku jest wysłanie ważnego sygnału ostrzegawczego do klientów – zastanawia się Katarzyna Szymielewicz. ©