Rzeczpospolita z 21.04.2017

Dane osobowe: Skutki przetwarzania, ocena zagrożeń i ryzyka, zasady profilowania

Jarosław Kamiński, adwokat Warszawa, Rödl & Partner

Trzynaście miesięcy pozostało przedsiębiorcom na dostosowanie przetwarzania danych osobowych w ich firmach do nowych unijnych przepisów. Warto już zacząć szkolenie pracowników, aby ich stosowanie było bezproblemowe.

Rozporządzenie Parlamentu Europejskiego i Rady o ochronie danych z kwietnia 2016 roku (RODO) zacznie obowiązywać od 25 maja 2018 roku.
Wprowadzono zupełnie nowe podejście do ochrony danych osobowych. Pojawi się przede wszystkim obowiązek administratora danych samooceny pod kątem oszacowania skutków przetwarzania dla ochrony danych i ewentualnego ryzyka (z angielskiego: risk-based approach). Obejmie on weryfikację przetwarzanych danych, ocenę zagrożeń związanych z przetwarzaniem konkretnych danych osobowych oraz planowane środki, zabezpieczenia i mechanizmy w celu zminimalizowania zagrożeń.

Ocenę skutków dla ochrony danych trzeba będzie przeprowadzić przed rozpoczęciem ich przetwarzania. Będzie ona obowiązkowa w dwóch przypadkach. Po pierwsze, gdy charakter, zakres, kontekst i cele danego rodzaju przetwarzania z dużym prawdopodobieństwem mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Po drugie, gdy decyzją organu nadzoru (np. GIODO) dany rodzaj operacji przetwarzania podlega obowiązkowej ocenie.

Profilowanie

Rozporządzenie reguluje zasady profilowania. W przepisach pojawia się legalna definicja tego pojęcia. W myśl przepisów profilowanie oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu tych danych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.
Profilowanie będzie legalne, gdy:
- wyraźnie dopuszcza to prawo
- jest niezbędne do zawarcia i wykonania umowy między osobą, której dane dotyczą, a administratorem danych
- osoba, której dane dotyczą, wyraziła zgodę.

Prawo do bycia zapomnianym

Nowe przepisy zwiększają uprawnienia osób, których dane dotyczą. Będą one miały nie tylko prawo dostępu do informacji (wglądu w dane), sprostowania danych, ograniczenia przetwarzania, ale także „prawo do bycia zapomnianym". Ma to polegać na tym, że klient będzie mógł żądać od administratora niezwłocznego usunięcia dotyczących go danych. Co więcej, w przypadku upublicznienia danych, to na administratorze danych osobowych będzie ciążył obowiązek podjęcia działań, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy usunęli wszelkie łącza do jego danych, ich kopii lub ich replikacji.
Klient będzie mógł też zwrócić się z żądaniem, by jego dane osobowe zostały przesłane przez administratora bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe. Chodzi o sytuację, gdy np. klient zmienia operatora sieci komórkowej i żąda, aby dotychczasowy operator przesłał dane nowemu operatorowi.

Odpowiedzialność i kary

Rozporządzenie przewiduje odpowiedzialność za naruszenie przepisów RODO zarówno o charakterze cywilnoprawnym, jak i administracyjnym.
Odpowiedzialność cywilnoprawna będzie dotyczyła każdej osoby, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia przepisów rozporządzenia. Będzie miała ona prawo uzyskać od administratora lub

podmiotu przetwarzającego odszkodowanie za poniesioną szkodę. Przy czym w przypadku przetwarzania danych przez więcej niż jednego administratora lub podmiotu przetwarzającego – odpowiedzialność będzie solidarna. Podmiotowi, który zapłacił całe odszkodowanie przysługiwać będzie prawo żądania od pozostałych administratorów lub podmiotów przetwarzających, którzy uczestniczyli w tym samym przetwarzaniu, zwrotu części odszkodowania odpowiadającej części szkody, za którą ponoszą odpowiedzialność.
Z kolei odpowiedzialność administracyjna ma się sprowadzać do kar pieniężnych nakładanych przez organ nadzorczy.

Zdaniem eksperta
Jarosław Kamiński, adwokat z kancelarii Rödl & Partner

Ogólne rozporządzenie o ochronie danych będzie wymagać od przedsiębiorców podjęcia szeregu działań i wdrożenia nowych procedur zarówno prawnych jak i informatycznych, m.in:
- weryfikacji przesłanek i podstaw przetwarzania danych osobowych;
- weryfikacji konieczności i zasadności powołania inspektora ochrony danych;
- analizy i weryfikacji dokumentacji kadrowej i zasad procesu rekrutacji;
- przeprowadzenia szkoleń dla pracowników;
- weryfikacji umów powierzenia przetwarzania danych osobowych oraz klauzul informacyjnych i klauzul zgody na przetwarzanie danych na gruncie RODO;
- opracowania dokumentacji związanej z ochroną danych na gruncie RODO (np. analiza ryzyka) oraz systematycznej (np. raz na kwartał/pół roku) jej weryfikacji.
Z kolei, w kontekście systemów IT szczególne znaczenie będzie miała dogłębna analiza ryzyka związana z ewentualnymi incydentami upublicznienia lub utraty danych, które trzeba będzie ocenić na podstawie aktualnego stanu wiedzy technicznej i znajomości realnych zagrożeń. Wzorcowo wdrożony proces analizy zagrożeń powinien uwzględniać także stałe monitorowanie informacji o wykrytych lukach w bezpieczeństwie systemów i aplikacji, a także umożliwiać szybką reakcję na pojawiające się zagrożenia o wysokim stopniu ryzyka dla bezpieczeństwa danych. Wyzwaniem staje się zatem także wdrożenie takich środków technicznych i organizacyjnych (formalnych), które w najlepszy możliwy sposób chroniłyby dane osobowe przed incydentami związanymi z ich bezpieczeństwem. Dobór tych środków spocznie w całości na przedsiębiorcach. Co więcej, dużą zmianą dla przedsiębiorców może być wprowadzenie obowiązku monitorowania incydentów związanych z bezpieczeństwem przetwarzanych danych. Administrator będzie miał jedynie 72 godziny na zgłoszenie organowi nadzorczemu wykrytego wycieku danych, włączając w to czas potrzebny na konieczną analizę skali problemu, określenie liczby i rodzaju danych, które wyciekły. Jeżeli zaś wyciek mógłby skutkować „wysokim ryzykiem naruszenia praw lub wolności osób fizycznych", to administrator będzie miał obowiązek poinformowania o zagrożeniu także poszczególnych osób, których to dotyczy. Co więcej, konieczne będzie także podniesienie poziomu świadomości zagrożeń wśród pracowników tak, aby ewentualny incydent został w ogóle rozpoznany i niezwłocznie zgłoszony administratorowi.
podstawa prawna: Rozporządzenie 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)

Co wpłynie na karę

Przy nakładaniu kar i określaniu ich wysokości organ weźmie pod uwagę:
- charakter, wagę i czas trwania naruszenia przy uwzględnieniu charakteru, zakresu lub celu danego przetwarzania, liczby poszkodowanych osób, których dane dotyczą oraz rozmiaru poniesionej przez nie szkody;
- umyślny lub nieumyślny charakter naruszenia;
- działania podjęte przez administratora lub podmiot przetwarzający w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą;
- stopień odpowiedzialności administratora lub podmiotu przetwarzającego z uwzględnieniem środków technicznych i organizacyjnych wdrożonych przez nich na mocy art. 25 i 32;
- wszelkie stosowne wcześniejsze naruszenia ze strony administratora lub podmiotu przetwarzającego;
- stopień współpracy z organem nadzorczym w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków;
- sposób, w jaki organ nadzorczy dowiedział się o naruszeniu, w szczególności, czy i w jakim zakresie administrator lub podmiot przetwarzający zgłosili naruszenie;
- jeżeli wobec administratora lub podmiotu przetwarzającego, których sprawa dotyczy, zostały wcześniej zastosowane w tej samej sprawie środki, o których mowa w art. 58 ust. 2 – przestrzeganie tych środków;
- stosowanie zatwierdzonych kodeksów postępowania na mocy art. 40 lub zatwierdzonych mechanizmów certyfikacji na mocy art. 42 oraz
- wszelkie inne obciążające lub łagodzące czynniki mające zastosowanie do okoliczności sprawy, takie jak osiągnięte bezpośrednio lub pośrednio w związku z naruszeniem korzyści finansowe lub uniknięcie straty.

Wysokość kary została uzależniona od rodzaju naruszenia i wynosić będzie nawet do 20 mln euro, a w przypadku przedsiębiorstwa – w wysokości do 4 proc. jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego.

Kogo dotyczy RODO

Obowiązek przetwarzania danych osobowych zgodnie z nowymi przepisami będzie spoczywać na:
- administratorach danych mających siedzibę na terenie UE, niezależnie od tego, czy przetwarzanie ma miejsce w UE;
- administratorach danych nie mających siedziby na terenie UE, którzy przetwarzają dane osób przebywających w UE, jeżeli:
– ma to związek z oferowaniem produktów lub usług osobom przebywającym w UE, bez względu na fakt odpłatności lub jej braku,
– monitorowane jest zachowanie osób przebywających w UE, o ile ich zachowanie ma miejsce na terenie UE (np. przeglądarki internetowe, Google),
- administratorach danych nie mających siedziby na terenie UE, ale posiadających jednostkę organizacyjną w miejscu, gdzie na podstawie prawa międzynarodowego ma zastosowanie prawo kraju członkowskiego UE.
Źródło: http://www.rp.pl/Firma/304219988-Dane-osobowe-Skutki-przetwarzania-ocena-zagrozen-i-ryzyka-zasady-profilowania.html#ap-4