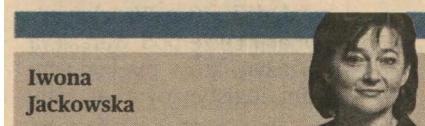


Dane osobowe po

PRAWO Każdy sposób zapewnienia danym bezpieczeństwa będzie do przyjęcia, ale gdy coś pójdzie nie tak, pobłażania nie będzie. Niedopatrzenie może kosztować nawet 20 mln EUR



► **OCZEKIWANIE NA OGŁOSZENIE:** Unijna reforma zacznie obowiązywać za dwa lata. Dr Edyta Bielak-Jomaa, generalny inspektor ochrony danych osobowych, spodziewa się, że rozporządzenie, które wprowadzi zmiany w całej Unii, najprawdopodobniej w czerwcu zostanie opublikowane w Dzienniku Urzędowym UE. [FOT. WM]



Iwona
Jackowska

i.jackowska@pb.pl ☎ 22-333-99-99

Unijna reforma ochrony danych osobowych czeka już tylko na formalny start. Obejmie wszystkie kraje członkowskie Unii Europejskiej (UE) i dla wielu przedsiębiorców będzie prawdziwym wyzwaniem.

Tę reformę wprowadzi rozporządzenie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych. I jak wszystkie rozporządzenia wspólnotowe, musi być stosowane bezpośrednio, stając się częścią krajowego porządku prawnego. Obecnie trwają prace nad odpowiednimi wersjami językowymi treści rozporządzenia, ostatecznie zaakceptowanego w grudniu 2015 r. Polska wersja jest konsultowana z Generalnym Inspektorem Ochrony Danych Osobowych (GIODO).

Jak przewiduje GIODO, Rada UE powinna w tym miesiącu formalnie przyjąć rozporządzenie we wszystkich wersjach językowych.

– Spodziewamy się, że w maju przyjmie je Parlament Europejski, a w czerwcu rozporządzenie zostanie opublikowane w Dzienniku Urzędowym UE i niedługo potem wejdzie w życie. W praktyce zacznie obowiązywać

dwa lata później – mówi generalny inspektor dr Edyta Bielak-Jomaa.

Plusy dla małych, dużych i klientów

Rozporządzenie ujednolici w UE nie tylko zasady ochrony danych, ale też procedury w postępowaniu krajowych organów nadzoru czy składaniu do nich skarg. Jednocześnie zwolni ono z części obowiązków niektóre firmy. Stawiane przedsiębiorstwom wymagania uzależnia bowiem od ich wielkości i rodzaju prowadzonej działalności. Przykładowo, jak informuje ODO 24, małe firmy nie będą musiały powoływać inspektora ochrony danych ani dokumentować czynności przetwarzania danych, które będą nowymi nieznanymi dotychczas obowiązkami. W ocenie ekspertów ODO 24, pozytywnych zmian jest więcej, dotyczą nie tylko małych przedsiębiorców, ale też grup kapitałowych. Jak mówi Leszek Kępa, przyszłe przepisy ułatwią im np. międzynarodową wymianę.

– Obserwujemy na co dzień, jak dużo problemów stwarza powierzanie i udostępnianie danych w grupach kapitałowych. Rozporządzenie unijne będzie obowiązywało bezpośrednio we wszystkich krajach członkowskich UE. Dla dużych, międzynarodowych grup kapitałowych, takich jak BMW, będzie to duże ułatwienie. Centralizację przepisów i możliwość wprowadzenia jednolitych zasad przetwarzania danych osobowych w międzynarodowych korporacjach

odbieramy bardzo pozytywnie – ocenia Aleksandra Chrzanowska, compliance officer w BMW Financial Services Polska.

Do tej reformy trzeba przygotowywać się już – organizacyjnie i finansowo. Nowe wymagania ochrony danych osobowych w wielu przypadkach oznaczają wydatki i wbrew pozorom nie tylko na nowe systemy informatyczne albo ich zmianę czy programy zabezpieczające dostęp do posiadanych zbiorów i chroniące je przed wyciekiem informacji.

– Już nie dwa czy trzy zdania będą liczyły informacje, które firmy będą musiały przekazywać swoim klientom przy zbieraniu od nich danych. Nowe wymagane klauzule mogą zająć pół strony, a niekiedy więcej – mówi Marcin Lewoszewski, radca prawny w zespole prawa nowych technologii kancelarii CMS.

Klient ma być powiadomiony nie tylko o celu przetwarzania jego danych, podstawie prawnej i możliwości cofnięcia na to zgody, co jest obowiązkiem również obecnie. Przedsiębiorca będzie musiał również np. podać okres, przez który zamierza przechowywać dane lub określić kryteria ustalania tego okresu. Do tego należy dostosować formularze służące do ich zbierania.

– Katalog tych informacji jest dość długi, znacznie szerszy niż obecnie i to na pewno zwiększy np. koszt wydruku dokumentów dla klientów. Szczególnie odczują to duże przedsiębiorstwa, na co dzień korespondu-

d ścisłą ochroną

jące z wieloma odbiorcami swoich usług i dla których dane osobowe są niemal podstawą działalności, czyli np. banki, towarzystwa ubezpieczeń, firmy pożyczkowe, telekomunikacyjne. Jednocześnie więcej będzie ich kosztowało przechowywanie dokumentacji – podkreśla radca.

Usługi zewnętrzne do weryfikacji

Jednak znacznie więcej wyzwań czeka przedsiębiorców, którzy powierzają przetwarzanie danych firmom zewnętrznym, tzw. dostawcom usług. Unijne rozporządzenie nakłada obowiązek zachowania szczególnej staranności przy ich wyborze, tylko podmioty gwarantujące najwyższy poziom ochrony danych osobowych mogą je przetwarzać w cudzym imieniu. To oznacza konieczność podjęcia działań przez obie strony. Korzystający z takich usług będą musieli zweryfikować obecne umowy i może nawet postawić nowe warunki partnerom czy wręcz ich zmienić. A usługodawcy, czyli centra danych i firmy wyspecjalizowane w ich analizie muszą zadbać o większą ochronę.

– Te firmy będą musiały zastosować wyszukane, bardziej skomplikowane środki bezpieczeństwa. Można zakładać, że wzrosną ceny usług tam, gdzie dane osobowe stanowią istotny element działalności, w szczególności przechowywania czy analizy danych. Ta sytuacja niewątpliwie wpłynie na konkurencję – prognozuje Marcin Lewoszewski.

Radca zwraca też szczególną uwagę na odpowiedzialność pracodawców za przetwarzanie danych pracowniczych przez zewnętrzne firmy. Gdy takie informacje stamtąd wyciekną, konsekwencje dotkną także pracodawcy zlecającego obsługę kadrową czy księgową biur w tym wyspecjalizowanym. Sankcje mogą być dotkliwe.

Unijne rozporządzenie przewiduje bardzo wysokie kary za niedochowanie należytej staranności przy przetwarzaniu danych osobowych. To nawet 20 mln EUR albo 4 proc. światowego rocznego obrotu, zależnie od tego, która z tych wartości okaże się wyższa. Jednocześnie nowe przepisy nie narzucają żadnych reguł technicznych ochrony danych.

Bezpieczeństwo i odpowiedzialność

– Obecnie polskie prawo precyzyjnie określa minimalny poziom środków bezpieczeństwa. Jest dość jasny, precyzyjny i raczej łatwy do zastosowania. Rozporządzenie unijne to zmieni, przerzuci na przedsiębiorców obowiązek oceny, czy stosowane przez nich zabezpieczenia zapewniają właściwą ochronę. Ustawodawca wspólnotowy pozwala na elastyczność działań, ale wymaga od przedsiębiorców pewnej dojrzałości. Daje sygnał: zastosuj sposób, jaki chcesz, byle był on skuteczny, a jeśli coś się stanie, odpowiesz za to – mówi Marcin Lewoszewski.

W nowych przepisach położono na ochronę prywatności duży nacisk.

– Trzeba będzie przykładąć dużo większą wagę do bezpieczeństwa danych, w tym być może również więcej inwestować w technologie – podkreśla Maciej Kaczmarek, prezes zarządu ODO 24.

Jak podają eksperci ODO 24, przy projektowaniu systemów ochronnych trzeba będzie wdrażać takie środki, by od samego początku właściwie chronić przetwarzane dane oraz prywatność osób, których one dotyczą. Dlatego np. ustawienia aplikacji czy serwisów społecznościowych domyśl-

Najważniejsze zmiany

Jak podaje ODO 24, najważniejsze zmiany to:

- **Preambuła** – niewiele aktów prawnych ją zawiera, ten wstęp w unijnym rozporządzeniu wyjaśni powody wprowadzania określonych przepisów, ma charakter legalnej wykładni.
- **Przetwarzanie danych przez grupy przedsiębiorstw** – będzie możliwe przetwarzanie danych wspólnie dla określonych celów, obecnie każdy administrator działa odrębnie, dzięki nowym przepisom współadministratorzy podzielą się obowiązkami, łatwiej też przetwarzać dane w grupach kapitałowych, w tym prowadzić międzynarodową wymianę.
- **Rejestr przetwarzania** – przedsiębiorcy mają dokumentować czynności przetwarzania, nie będą już musieli rejestrować zbiorów, w razie stwierdzenia w firmie, że istnieje duże zagrożenie dla ochrony prywatności, przed rozpoczęciem przetwarzania powinni zwrócić się o poradę do GODO.
- **Inspektor zamiast ABI** – nazwa administratora bezpieczeństwa informacji (ABI) zostanie zastąpiona inspektorem ochrony danych, ma on ściśle współpracować z GODO, z inspektorem będą mogły kontaktować się osoby, których dane są pod jego opieką przetwarzane.
- **Wymagania dopasowane do przedsiębiorstwa** – zależeć będą od jego wielkości i rodzaju działalności, w małych firmach nie trzeba będzie powoływać inspektora ochrony danych i prowadzić tzw. rejestru przetwarzania.
- **Zgłaszanie wycieku danych do GODO** – administrator będzie miał na to 72 godziny, w razie poważnego naruszenia poinformuje o tym też osoby, których dane są przetwarzane.
- **Ochrona prywatności** – ustawienia aplikacji czy serwisów społecznościowych powinny udostępniać minimalną ilość danych, tylko użytkownik będzie mógł poszerzyć ich zakres.
- **Łatwiejsze składanie skarg** – składanie skarg będzie darmowe, obecnie w Polsce opłata skarbową wynosi 10 zł, skargę będzie można złożyć organowi nadzoru w dowolnym kraju.
- **Wysokie kary** – sankcje za nieprzestrzeganie przepisów dotyczących ochrony danych mogą sięgać 20 mln EUR lub 4 proc. światowego obrotu przedsiębiorstwa, kara ma zależeć m.in. od stopnia winy, naprawienia (lub nie) szkody, czy już zdarzały się podobne sytuacje.

nie powinny udostępniać minimalną ilość informacji o użytkowniku, a poszerzenie ich zakresu może wynikać jedynie z ustawień dokonanych przez samego użytkownika. Obecnie takie zagadnienia nie są uregulowane w polskim prawie.

Zdaniem Aleksandry Chrzanowskiej z BMW Financial Services Polska, w przygotowaniu się polskich firm do wejścia w życie unijnego rozporządzenia jest bardzo pomocna nowelizacja polskiej ustawy o ochronie danych osobowych, która zaczęła obowiązywać w styczniu 2015 r. – przez dużą zbieżność wymogów krajowych z zapowiadany zmianami. Jednocześnie jednak, mimo istnienia w Polsce od wielu lat przepisów regulujących ochronę danych osobowych, zauważa ona niską tego świadomość wśród przedsiębiorców.

– W Polsce, niestety, wciąż istnieje ten problem. Dlatego tak ważna jest edukacja biznesu i podnoszenie samoświadomości przedsiębiorców w dziedzinie ochrony danych osobowych. W dojrzałych organizacjach, w których sprawnie działa ABI, powołanie inspektora ochrony danych, zbieranie pozwoleń od klientów wraz z zastosowaniem nowych klauzul informacyjnych nie będzie stanowiło większego zaskoczenia – ocenia Aleksandra Chrzanowska.

Jak przewiduje, podobnie będzie z przeprowadzaniem w takich firmach analizy ryzyka i wdrażaniem oceny skutków przedsięwzięcia dla ochrony prywatności, czyli PIA (Privacy Impact Assessment).

Marcin Lewoszewski z CMS zwraca uwagę, że reforma ochrony danych osobowych jest tak znacząca, że w każdej większej firmie warto rozważyć powołanie zespołu do wdrożenia reguł wynikających z nowych wymagań.

– Zmian będzie dużo i mogą wiązać się z dużymi kosztami. Dostosowanie do nich nie może przebiegać ani szybko, ani tanio. I jedna osoba do tego nie wystarczy – stwierdza radca prawny. © ®

Informacje dla klienta

Podczas pozyskiwania danych od osoby fizycznej administrator będzie musiał jej przekazać m.in. następujące informacje:

- swoją tożsamość, dane kontaktowe, tożsamość i dane kontaktowe swojego przedstawiciela i inspektora ochrony danych,
- cele przetwarzania i jego podstawę prawną,
- omówienie tzw. uzasadnionych interesów przetwarzania, jeżeli ma być prowadzone na podstawie takich interesów realizowanych przez administratora lub przez stronę trzecią,
- w określonych przypadkach informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, a także o zamiarze przekazania danych do państwa trzeciego,
- okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
- informacje o uprawnieniach osoby, której dotyczą dane, takich jak np. prawo do dostępu do własnych danych, ich poprawienia, usunięcia, ograniczenia przetwarzania, wniesienia sprzeciwu wobec przetwarzania danych, do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem czy do skargi,
- informację, czy podanie danych jest wymogiem ustawowym lub umownym albo warunkiem przystąpienia do umowy oraz czy podmiot danych jest zobowiązany do ich podania i jakie są ewentualne konsekwencje niepodania danych,
- informację, że firma prowadzi automatyczne podejmowanie decyzji (w tym profilowanie), informacje o trybie jego działania, jego znaczeniu i przewidywanych konsekwencjach.