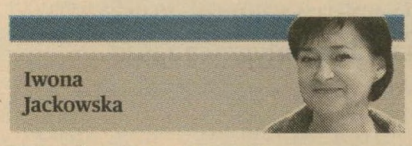
RODO: zaczyna się egzam

Nowe prawo To nie rewolucja, a ewolucja – tak szefostwo organu nadzorującego ochronę danych osobowych ocenia obowiązujące od dziś zmiany



Iwona Jackowska

i.jackowska@pb.pl ☎ 22-333-98-59

Wybiła godzina zero dla reformy ochrony danych osobowych. Od dziś w całej Unii Europejskiej, a więc i w Polsce, należy stosować jednolite jej zasady. Musi ich przestrzegać każdy podmiot, który przetwarza informacje dotyczące osób fizycznych, czyli je zbiera, utrwala, organizuje, porządkuje, przechowuje, adaptuje i modyfikuje, pobiera, przegląda, wykorzystuje, rozpowszechnia, łączy, przesyła lub niszczy – zarówno w sposób zautomatyzowany, jak i niezautomatyzowany. Tak definiuje operacje przetwarzania unijne Ogólne Rozporządzenie o Ochronie Danych Osobowych 2016/679 (RODO), które wyznacza nowe standardy dbania o czyjąś prywatność.

RODO jest od 25 maja tego roku podstawowym aktem regulującym zasady ochrony danych osobowych i w każdym państwie UE musi być ono traktowane jak prawo krajowe, stosowane bezpośrednio .

Wbrew pozorom nie każda informacja podlega wymogom RODO. Nie każda też musi być pozyskana przez dany podmiot, aby mógł realizować działalność, w której uzyskanie danych osobowych jest konieczne. Ważny jest cel ich przetwarzania, jak mówi dr Edyta Bielak-Jomaa, prezes Urzędu Ochrony Danych Osobowych (UODO), a do wczoraj, przed reformą – Generalny Inspektor Ochrony Danych Osobowych (GIODO).

Definicja danych

– Czy w zakładzie fryzjerskim dla umówienia terminu wykonania usługi i omówienia jej szczegółów konieczna jest wiedza np. o tym, gdzie mieszka klient? Wystarczy zapewne zapisać tylko jego imię, ewentualnie numer telefonu na wypadek koniecznego odwołania zaplanowanej wizyty czy zmiany jej godziny – wyjaśnia prezes organu nadzoru.

Zgodnie z RODO dane osobowe to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Ta ostatnia to taka, którą można bezpośrednio lub pośrednio określić, w szczególności na podstawie imienia i nazwiska, numeru identyfikacyjnego, danych o lokalizacji, identyfikatora internetowego lub jednego bądź kilku szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość.

To w zasadzie nic nowego w porównaniu z definicją znaną z ustawy o ochronie danych osobowych obowiązującą od 20 lat, która dziś utraciła moc. Swego czasu organ nadzoru wyjaśniał, że nie uważa się określonej informacji za umożliwiającą ustalenie czyjejś tożsamości, jeżeli wymagałoby to nadmiernych kosztów, czasu i działań. Może być nią informacja uzyskana bez nadzwyczajnego wysiłku i nakładów, zwłaszcza przy wykorzystaniu łatwo osiągalnych i powszechnie dostępnych źródeł. W ocenie GIODO, można było przyjąć, że danymi osobowymi nie są pojedyncze informacje o dużym stopniu ogólności, np. nazwa ulicy i numer domu czy wysokość wynagrodzenia, ale staną się nimi, gdy ktoś je zestawi z innymi, dodatkowymi, które można odnieść do konkretnej osoby. Jednak, uwaga: numer PESEL to już dana osobowa – co prawda wyrażona pojedynczo, ale zawierająca datę urodzenia i płeć.

Jak wykorzystywać zbiory

Dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty – to jedna z podstawowych zasad RODO. Również wspomniane pozyskiwanie informacji odpowiednie do potrzeb prowadzonej działalności jest obowiązkiem płynącym wprost z tego rozporządzenia. Wręcz nakazuje, aby zbierano tylko adekwatne, stosowne i ograniczone do tego, co niezbędne i celów, do których będą wykorzystywane. Unijny akt zaleca tzw. minimalizację danych, co dr Edyta Bielak-Jomaa wskazuje m.in. jako zaletę z punktu widzenia chociażby kosztów ponoszonych przez administratorów danych osobowych (ADO) czy firm przetwarzających zbiory informacji na zlecenie ADO, czyli tzw. procesorów. Wszelkie te operacje, zgodnie z RODO, muszą odbywać się zgodnie z zasadą integralności i poufności – to znaczy w sposób zapewniający odpowiednie zabezpieczenie danych osobowych, w tym przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem za pomocą odpowiednich środków technicznych lub organizacyjnych. Jednocześnie unijny prawodawca nie wskazuje norm, jakie te rozwiązania powinny spełniać. Przedsiębiorcy nie znajdą też w polskich przepisach – ani w ustawach, ani w aktach wykonawczych – takich kryteriów. Obecnie panuje pod tym względem dowolność – wybór należy do administratora. Jednocześnie jednak, jako odpowiedzialny za stosowanie przepisów, musi on być w stanie wykazać, że ich przestrzega. To następna reguła unijnej reformy – zasada rozliczalności.

Wolny wybór metod

Swoboda co do stosowania zabezpieczeń ma przede wszystkim ten plus, że administrator może wybrać rozwiązania najkorzystniejsze ze swojego punktu widzenia. Nie może przy tym zapominać, że ochrona nie sprowadza się jedynie do wdrożenia odpowiedniego systemu informatycznego, korzystania z oprogramowania w chmurze czy zamykania informacji w szafach z cyfrowym zamkiem. Ważne są też procedury i właściwe zachowania zatrudnionych ludzi.

– Np. upoważnienia dostępu do zbiorów danych dla osób je przetwarzających muszą być skrupulatnie przyznawane. Ale powinny być także na bieżąco ewidencjonowane, co bez problemu można rejestrować, także w systemie informatycznym – mówi Katarzyna Jaśniewicz, menedżer w Unit4 Polska.

Jej zdaniem, przedsiębiorcy, dostosowując środowisko informatyczne do RODO, powinni wziąć pod uwagę wspomnianą minimalizację przetwarzania danych. Warto wyodrębniać w systemach określone działy, np. związane z zakresem obowiązków pracowników przetwarzających dane osobowe – jedne dotyczące urlopów, a inne chociażby szkoleń. I podobnie budować zbiory informacji pochodzących od klientów czy kontrahentów.

Jednak, jak wielokrotnie wskazywano w ostatnich miesiącach, dobre zabezpieczenie przed ryzykiem wycieku danych czy ich zniszczenia zależy nie tylko od ludzi, którzy otrzymali dostęp do przetwarzania danych. Pracownicy powinni wiedzieć, że nawet odchodząc od biurka i zostawiając odblokowany komputer, mogą stworzyć możliwość włamania się do cennych informacji przez nieupoważnioną do tego osobę. Nie wszędzie jest to takie oczywiste, jak podkreśla Maciej Jurczyk, inżynier ds. bezpieczeństwa informacji w ODO 24, po doświadczeniach z audytów wdrożeniowych przeprowadzanych w różnych firmach.

Wątpliwości bez liku

Marcin Czarnecki, konsultant ds. rozwoju biznesu w Konica Minolta Business Solutions Polska, zwraca uwagę, że w przygotowaniach do nowych wymagań problemów przysporzyła firmom przede wszystkim interpretacja przepisów. Z badania firmy, opublikowanego w pierwszym kwartale roku, wynika, że 43 proc. spółek zatrudniających do 50 pracowników nie ma wystarczającej wiedzy o RODO i sposobach przygotowania się do zmian.

– Przedsiębiorcy mieli wątpliwości, czy rozporządzenie dotyczy ich działalności. Nie zdawali sobie sprawy, jakie konkretnie dane muszą chronić i w jaki sposób powinni to robić. Nowe przepisy nie narzucają konkretnych rozwiązań, dlatego każda firma musiała je opracować. Niektóre potrzebowały usprawnienia systemu cyberbezpieczeństwa, przeprowadzenia migracji do chmury, zakupu dodatkowego wyposażenia czy reorganizacji biura – wyjaśnia Marcin Czarnecki.

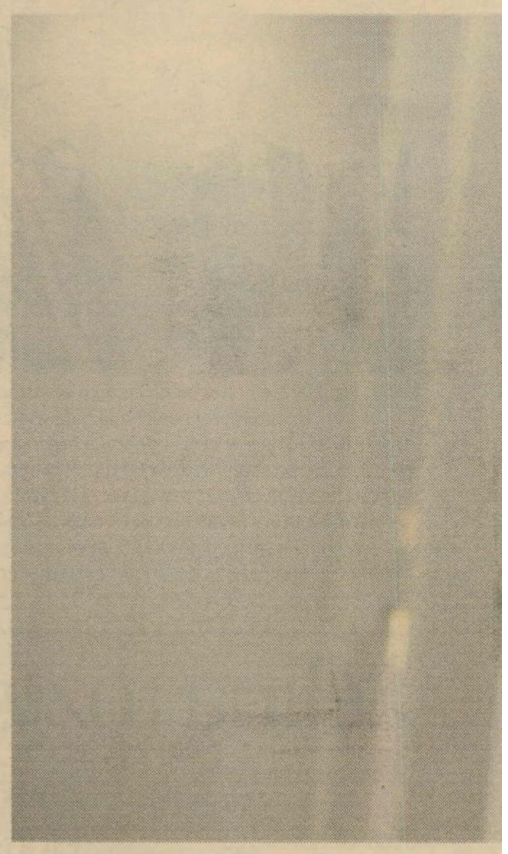
Dodaje, że przedsiębiorcy musieli również zweryfikować partnerów, którym ich firma przekazuje dane osobowe, i podpisać odpowiednie umowy powierzenia.

– Pełniąc rolę administratora, przedsiębiorca powinien sprawdzić, czy wszystkie podmioty, z którymi współpracuje, działają

Informacje dla klienta

Przedsiębiorca przy zbieraniu danych musi przekazać osobie, od której je pozyskuje, następujące informacje:

- swoją tożsamość i dane kontaktowe — własne, a także inspektora ochrony danych, jeżeli został powołany,
- o celu przetwarzania danych osobowych i podstawy prawnej do tego,
- o odbiorcach danych lub ich kategoriach,
- o zamiarze transferu danych do państwa trzeciego,
- o okresie przechowywania danych, a gdy nie można go sprecyzować, kryteria jego ustalenia,
- o prawie żądania od administratora dostępu do swoich danych, ich sprostowania, usunięcia, ograniczenia przetwarzania lub o prawie do sprzeciwu wobec przetwarzania i uprawnieniu do przenoszenia danych,
- o prawie do cofnięcia w dowolnym momencie udzielonej zgody na przetwarzanie,
- o prawie wniesienia skargi do organu nadzorczego,
- o tym, czy podanie danych osobowych jest wymogiem ustawowym, umownym lub warunkiem zawarcia umowy, i czy osoba, której one dotyczą, ma obowiązek ich przedstawienia i co oznacza dla niej niewywiązanie się z tego,
- o zautomatyzowanym podejmowaniu decyzji, zasadach tego i konsekwencjach dla klienta, w tym o profilowaniu, jeśli jest ono stosowane.



JAKA WINA, TAKA KARA: Dr Edyta Bielak-Jomaa, prezes Urzędu Ochrony Danych Osobowych, uważa, że groźba kar za niezachowanie odpowiedniej ochrony danych skłoniła firmy do przykładania większej wagi do przestrzegania nowych zasad, co przekłada się na zwiększenie bezpieczeństwa przetwarzanych tych informacji. Jednocześnie zapowiada, że kary będą współmierne do przewinienia, skali nieprawidłowości i postawy administratorów wobec powstałego ryzyka naruszeń praw i wolności. [FOT. WM]

in praktyczny

Obowiązki ADO nie sprowadzają się jednak wyłącznie do dbałości o zabezpieczenie posiadanych zbiorów przed ryzykiem ich utraty czy dostępu do nich przez nieuprawnione osoby czy firmy. Ma on za zadanie uświadomić zainteresowanych, po co je przetwarza i co to dla nich oznacza. RODO zawiera długi katalog informacji, które należy przekazać każdemu, od kogo dane są pozyskiwane, w tym o prawie do bycia zapomnianym, czyli do żądania całkowitego ich usunięcia, gdy np. nie ma podstaw do dalszego ich przetwarzania lub gdy ktoś wycofał swoją uprzednią zgodę na to. Dla przedsiębiorców oznacza to nie tylko usunięcie wszystkich informacji dotyczących danej osoby, także będących w posiadaniu innych podmiotów, czyli wszelkich łączy do danych, kopii, korespondencji elektronicznej, jakichkolwiek zbiorów przechowywanych w papierowej formie, wydruków e-maili. To ogromne wyzwanie dla firm, które po otrzymaniu takiego żądania muszą je spełnić bez zbędnej zwłoki.

Przedsiębiorcy nie muszą już zgłaszać posiadanych zbiorów organowi nadzoru, ale muszą rejestrować czynności z nimi związane. Z obowiązku tego są zwolnieni mali i średni przedsiębiorcy, zatrudniający do 250 pracowników, jeżeli nie wykorzystują np. informacji wrażliwych, a przetwarzanie danych ma charakter sporadyczny i nie stwarza ryzyka naruszenia ważnych praw osób.

Rejestrowanie czynności przetwarzania

RODO wymaga w art. 30 prowadzenia rejestru czynności przetwarzania danych osobowych. Należy podać w nim m.in. imię i nazwisko lub nazwę oraz dane kontaktowe administratora i współadministratorów, cele przetwarzania, opis kategorii osób i wykorzystywanych informacji, a także odbiorców, którym są lub będą ujawnianie, możliwy ogólny opis technicznych i organizacyjnych sposobów bezpieczeństwa.
Nie wszyscy muszą wywiązywać się z tego obowiązku. Zwolnieni są z niego przedsiębiorcy zatrudniający do 250 pracowników, ale pod określonymi warunkami. Przetwarzanie nie może powodować ryzyka naruszenia praw lub wolności, ma charakter sporadyczny i nie dotyczy danych wrażliwych oraz wynikających z wyroków skazujących i czynów zabronionych.

Powołanie inspektora ochrony danych

Powołanie przez administratora inspektora ochrony danych (IOD) — m.in. dbającego o właściwe stosowanie przepisów — nie jest obowiązkowe dla wszystkich podmiotów przetwarzających dane. Muszą go wyznaczyć m.in. podmioty publiczne. W sektorze prywatnym inspektor musi działać w firmach, w których przetwarzanie danych jest regularne i prowadzone na dużą skalę. RODO pozwala wybrać wspólnego IOD dla więcej niż jednej firmy.
Administratorzy muszą powiadomić organ nadzoru o powołaniu inspektorów do 31 lipca tego roku. W wielu przypadkach ich rolę będą pełnić dotychczasowi administratorzy bezpieczeństwa informacji (ABI). W takim przypadku powinni być zgłoszeni w UODO do 1 września 2018 r. W tym samym terminie należy powiadomić urząd, jeżeli funkcję IOD powierzono osobie innej niż dotychczasowemu ABI.

zgodnie z RODO. Jest to bardzo pracochłonny proces, zwłaszcza w przypadku większych firm – podkreśla Marcin Czarnecki.

Procesor pod kontrolą

Na powierzanie danych firmom świadczącym usługi kadrowe, księgowe czy serwisu IT na rzecz określonych przedsiębiorców i konsekwencje niewłaściwej ochrony przekazanych informacji zwraca uwagę także organ nadzoru. Piotr Drobek, dyrektor kierujący Zespołem Analiz i Strategii w UODO, podkreśla, że odpowiedzialność ponoszą obie strony, aczkolwiek, gdy dojdzie do naruszenia u procesora (np. wycieku danych), o incydencie urząd musi być poinformowany przez administratora – w ciągu 72 godzin od jego stwierdzenia, jak wynika z RODO.

Nie zawsze powiadomienie o takiej sytuacji będzie konieczne (jest wymagane przede wszystkim wtedy, gdy powstanie ryzyko naruszenia czyichś praw i wolności), jednak dla uniknięcia ryzyka ważne jest sprawdzenie podmiotu, któremu dane osobowe są przekazywane, pod kątem gwarancji bezpieczeństwa. RODO wręcz uprawnia do takiej kontroli, przy czym niedostosowanie umowy powierzenia do nowych zasad (np. brak określenia, czy dotyczy danych zwykłych, czy wrażliwych, charakteru i celu przetwarzania, czasu trwania tych procesów) może słono kosztować obie strony. Przewidziane w rozporządzeniu kary finansowe mogą sięgać 20 mln EUR lub 4 proc. wartości światowego rocznego obrotu firmy.

Naruszenia pod groźbą sankcji

Obowiązków zatem przybyło, jednak w ocenie kierownictwa organu nadzoru nowe wymagania nie są rewolucją w ochronie danych osobowych, a ewolucją. Mirosław Sanek, wiceprezes UODO, podkreśla, że wiele z jej wymagań jest znanych od lat, a na powszechny niepokój z wprowadzeniem RODO w dużej mierze wpłynął fakt, że przewiduje ono sankcje za naruszenia.

– Informacje na ten temat odegrały jednocześnie rolę edukacyjną. Badania opinii wśród firm pokazują, że ponad 60 proc. z nich zainteresowała się nowymi przepisami i podjęła działania, gdy usłyszała o groźbie kar. Chcę przy tym podkreślić, że określono kilkanaście przesłanek procedury ich nakładania i nie ma mowy o dowolnym ich wymierzaniu – mówi Mirosław Sanek.

Dr Edyta Bielak-Jomaa zapowiada, że każda decyzja organu nadzoru o karze będzie poprzedzona analizą stopnia winy.

– Trzeba będzie ocenić m.in. wagę naruszenia, czy było umyślne, czy nie, jak administrator albo podmiot przetwarzający dane współpracuje z organem dla złagodzenia skutków powstałej sytuacji oraz czy i co zrobił dla zminimalizowania szkód. Ponadto weźmiemy pod uwagę, czy wcześniej też dochodziło do podobnych zdarzeń – wyjaśnia prezes UODO.

Przedstawiciele urzędu zwracają uwagę, że sankcje nie są istotą ochrony danych osobowych i działalności tej instytucji. Nowa polska ustawa o ochronie danych osobowych, która dziś weszła w życie, nakłada na UODO wiele nowych zadań, w tym upowszechnianie wśród przetwarzających dane wiedzy o ich obowiązkach. Dostosowano do nich strukturę wewnętrzną organu. Powstały m.in. zespoły do spraw współpracy z administratorami i przetwarzania danych w sektorze prywatnym.