INFOR.PL
SEKTOR PUBLICZNY

Data publikacji: 25.01.2018

Jak przygotować się do zmian w systemie ochrony danych? - rozmowa dr Edytą Bielak–Jomaa, Generalnym Inspektorem Ochrony Danych Osobowych (GIODO)

RODO ma być neutralne technologicznie, elastyczne i dawać przedsiębiorcom większą swobodę działania, dlatego zawiera jedynie ogólne unormowania. Trzeba się do tej zmiany podejścia w ochronie danych osobowych przyzwyczaić i właściwie zorganizować procesy przetwarzania w swojej firmie czy instytucji.

Infor.pl: Bezpośrednią okazją do naszej rozmowy są obchody przypadającego na 28 stycznia Dnia Ochrony Danych Osobowych. W tym roku obchodzimy go po raz dwunasty. Celem tej inicjatywy jest m.in. zwiększanie świadomości na temat wagi ochrony naszej prywatności. Jak więc obecnie wygląda wiedza obywateli na ten temat – lepiej chronimy naszą prywatność i dane osobowe niż jeszcze kilka lat temu?

dr Edytą Bielak–Jomaa: W opinii GIODO, wiedza na temat ochrony danych osobowych stopniowo, ale wciąż się zwiększa. Świadczy o tym chociażby coraz większa liczba wpływających do nas skarg. Niemniej uważam, że nadal jest jeszcze wiele to zrobienia w tej kwestii. Bardzo zależy mi na tym, żeby Polacy nauczyli się widzieć związek przyczynowo-skutkowy między swoim zachowaniem a naruszaniem ich prywatności; żeby wiedzieli, kiedy mogą odmówić podania swoich danych, a kiedy nie; żeby mieli świadomość ryzyka kradzieży tożsamości i potrafili je minimalizować; żeby umieli wyznaczać granicę w udostępnianiu informacji; żeby pamiętali, iż przekazywane przez nich dane bywają gromadzone przez różne podmioty i często wykorzystywane w niezgodny z prawem i ich wolą sposób. Wiedza na ten temat wciąż jest zbyt mała.

Dlatego m.in. GIODO realizuje wiele przedsięwzięć o charakterze edukacyjnym. Jednym z ważniejszych jest program dla szkół „Twoje dane – Twoja sprawa", w którym obecnie uczestniczą aż 333 placówki edukacyjne. Celem tej inicjatywy jest podnoszenie świadomości na temat ochrony danych osobowych i prawa do prywatności zarówno wśród nauczycieli, jak i uczniów. Jest to o tyle istotne, że młode pokolenie jest pokoleniem informacyjnym, idealnie poruszającym się w nowościach technologicznych, ale ma ograniczoną wiedzę z dziedziny praw i obowiązków obywatelskich. Brak im też rozwagi, mądrości życiowej, roztropności, przewidywania konsekwencji swojego działania, co rodzi istotne zagrożenia. Dlatego podnoszenie poziomu ich świadomości oraz kształtowanie odpowiednich nawyków i zachowania w zakresie ochrony danych osobowych to ważne zadanie.

Cieszy mnie to, że szkoły i ośrodki doskonalenia nauczycieli w całej Polsce, przyłączając się do obchodów Dnia Ochrony Danych Osobowych, realizują wiele różnych przedsięwzięć edukacyjno-informacyjnych, takich jak: apele, teleturnieje, gry planszowe, gry miejskie, konkursy, autorskie przedstawienia, happeningi, spotkania, warsztaty czy pogadanki. Angażują one nie tylko całą społeczność szkolną - uczniów, nauczycieli, rodziców, ale także środowisko lokalne - mieszkańców miast i gmin oraz liczne urzędy.

Każdego roku przybywa również uczelni wyższych, które włączają się w obchody Dnia Ochrony Danych Osobowych. Organizowane wspólnie z GIODO konferencje i spotkania, które cieszą się dużym zainteresowaniem, są doskonałą okazją do szerzenia wiedzy z zakresu ochrony danych i prawa do prywatności.

Tematem przewodnim tegorocznych obchodów Dnia Ochrony Danych Osobowych jest ogólne rozporządzenie o ochronie danych osobowych (RODO), które za kilka miesięcy będzie bezpośrednio stosowane we wszystkich państwach Unii Europejskiej. Mówi się, że to rewolucja, a firmy w dużej mierze nie są do niej przygotowane. Czy jednak administrator danych, który dziś dopełnia wszystkich obowiązków związanych z przetwarzaniem danych, musi jakoś specjalnie szykować się do tych zmian?

Te podmioty, które już teraz rzetelnie podchodzą do przetwarzania danych osobowych i stosują obecnie obowiązujące zasady w tym zakresie, nie powinny mieć dużych problemów ze spełnieniem nowych wymogów.

Podstawowe rozwiązania ogólnego rozporządzenia o ochronie danych osobowych trudno bowiem uznać za rewolucyjne, w przeciwieństwie do zaprezentowanego w tym dokumencie podejścia do praktycznego zastosowania tych zasad. Nie zmieniają się bowiem w sposób istotny podstawy prawne czy zasady przetwarzania danych osobowych. Natomiast rewolucyjny charakter ma wprowadzenie nowych rozwiązań i regulacji, które zwiększają samodzielność, ale i odpowiedzialność administratorów danych.

Obecnie niezmiernie ważne jest jednak to, by administratorzy danych, zwłaszcza ci, którzy dotąd nie podejmowali żadnych działań w związku z reformą systemu ochrony danych osobowych, prowadzili intensywne prace związane z wdrożeniem nowych rozwiązań, nie czekając na jakiekolwiek zmiany w przepisach krajowych. Unijne rozporządzenie weszło w życie w 2016 roku, jedynie jego stosowanie jest odroczone do 25 maja 2018 roku. Natomiast wszystko, co jest związane z obowiązkami administratorów danych, z ich odpowiedzialnością oraz uprawnieniami - wynika wprost z rozporządzenia. Dlatego nie ma co czekać na dodatkowe uregulowania. Oczywiście, przepisy sektorowe są niezwykle istotne, ale one powinny być jedynie dostosowane do postanowień RODO. Natomiast jeśli chodzi o sam zrąb reformy, to on jest znany i już trzeba przygotowywać się do stosowania nowych regulacji.

Bardzo zależy mi też na tym, aby administratorzy danych uświadomili sobie, że rozporządzenie nie tylko nakłada na nich nowe obowiązki i zwiększa ich odpowiedzialność za przetwarzanie danych osobowych zgodnie z prawem, ale również zapewnia im większą elastyczność działania. Przykładowo, jeśli ktoś tradycyjnymi metodami przetwarza niewielki zakres danych osobowych, to nie będzie zobowiązany do stosowania skomplikowanych i kosztownych zabezpieczeń.

Co administratorzy muszą zrobić, by właściwie przygotować się do zmian w systemie ochrony danych?

Jeśli ktoś nie jest jeszcze w ogóle przygotowany do stosowania rozporządzenia, to jak najszybciej powinien podjąć niezbędne działania. Czasu na osiągnięcie zgodności z RODO jest bowiem coraz mniej, a odlicza go specjalny zegar umieszczony na stronie internetowej GIODO.

A co trzeba robić? Przede wszystkim dokonać przeglądu wszystkich procedur związanych z przetwarzaniem danych osobowych. Sprawdzić m.in., na jakiej podstawie prawnej są przetwarzane, czy są adekwatne do celów oraz aktualne. Należy też przeanalizować choćby to, czy zebrane dotychczas zgody na przetwarzanie danych osobowych będą ważne, gdy zaczniemy stosować RODO. Trzeba też się przygotować do szerszego i dokładniejszego informowania osób, których dane są przetwarzane. Warto przy tym pamiętać, że zgodnie z RODO, od administratorów danych wymagać się będzie, by wszelkie informacje kierowane do osób, których dane dotyczą, by były formułowane jasnym i prostym językiem, by były zwięzłe i zrozumiałe. Szczególnie istotne będzie to zaś wówczas, gdy informacje i komunikaty będą kierowane do dzieci, które muszą móc je bez trudu zrozumieć. Ponadto przystępując do prac nad różnymi projektami (np. systemami IT czy nowymi usługami), od samego początku trzeba uwzględniać ochronę danych osobowych, tak by z założenia pozyskiwać minimalny zakres danych, jaki jest niezbędny do osiągnięcia zakładanego celu.

Z tych i wielu innych obowiązków każdy administrator i podmiot przetwarzający musi być w stanie się rozliczyć, czyli wykazać, że dane są właściwie przetwarzane. Zatem przed każdym administratorem danych jest wiele pracy.

Żeby podmiotom zobowiązanym ułatwić przygotowanie się do stosowania nowych zasad przetwarzania danych osobowych, Generalny Inspektor Ochrony Danych Osobowych już jakiś czas temu przygotował publikację pt. „Czy jesteś gotowy na RODO?", zwracającą uwagę na najważniejsze zagadnienia i obszary, w których następować będą znaczące zmiany. Jest ona dostępna na stronie internetowej urzędu pod linkiem http://www.giodo.gov.pl/pl/1520281/10255. Zachęcam, by poddać się temu sprawdzianowi i ocenić swoją gotowość do stosowania RODO.

RODO nie zawiera gotowych zaleceń, których przestrzeganie automatycznie oznaczałoby właściwe realizowanie obowiązków ciążących na administratorach danych. Przedsiębiorcy często jednak potrzebują gotowych instrukcji, wzorów rozwiązań. Czy GIODO planuje ich przygotowanie?

RODO ma być neutralne technologicznie, elastyczne i dawać przedsiębiorcom większą swobodę działania, dlatego zawiera jedynie ogólne unormowania. Trzeba się do tej zmiany podejścia w ochronie danych osobowych przyzwyczaić i właściwie zorganizować procesy przetwarzania w swojej firmie czy instytucji.

GIODO od chwili oficjalnej prezentacji zmian, jakie Unia Europejska postanowiła wprowadzić w przepisach dotyczących ochrony danych osobowych (co miało miejsce w styczniu 2012 r.), podejmuje wiele inicjatyw mających na celu jak najlepsze przygotowanie wszystkich podmiotów do stosowania nowych regulacji. Między innymi wspiera wiedzą ekspercką poszczególne urzędy, prowadząc dla nich np. specjalne szkolenia dotyczące RODO (jak m.in. dla Ministerstwa Rozwoju czy Kancelarii Sejmu). Ponadto opiniując projekty wielu różnorodnych aktów prawnych, w każdym uzasadnionym przypadku zwraca uwagę na konieczność zapewnienia zgodności projektowanych przepisów z regulacjami zawartymi w ogólnym rozporządzeniu o ochronie danych.

Biorąc zaś pod uwagę to, że fachowa wiedza ABI (przyszłych inspektorów ochrony danych), jest fundamentem, na którym zbudować można system skutecznej ochrony danych osobowych danej instytucji, wspieranie ich kształcenia GIODO uznał za jeden z priorytetów. Stąd m.in. przygotowanie specjalnej publikacji „Wykonywanie obowiązków ABI, przyszłego inspektora ochrony danych, w świetle ogólnego rozporządzenia o ochronie danych" (dostępnej na stronie internetowej GIODO pod linkiem http://giodo.gov.pl/259/id_art/9760/j/pl) czy realizacja sektorowych szkoleń dla ABI, w których wzięło już udział ponad 1500 osób sprawujących tę funkcję.

Ponadto GIODO jako członek Grupy Roboczej Artykułu 29 - niezależnego europejskiego organu doradczego Komisji Europejskiej w zakresie ochrony danych osobowych i prywatności – wspólnie z innymi europejskimi rzecznikami ochrony danych przygotowuje wytyczne, które mają ułatwić administratorom danych zrozumienie i stosowanie konkretnych rozwiązań i instrumentów ogólnego rozporządzenia. Powstało już kilka tego typu dokumentów, a nad kolejnymi prace wciąż się toczą. Wszystkie te dokumenty są dostępne na stronie internetowej urzędu.

Ale jeśli rozmawiamy o wskazówkach związanych ze stosowaniem RODO, to chciałabym zwrócić uwagę na inny pomocny w tym zakresie instrument – kodeksy postępowania, którym GIODO poświęcił ostatnio specjalny warsztat informacyjno-szkoleniowy. Dokumenty te mogą być tworzone przez zrzeszenia oraz inne podmioty reprezentujące różne kategorie administratorów czy podmiotów przetwarzających. Ich celem jest doprecyzowanie postanowień rozporządzenia z uwzględnieniem specyfiki danego sektora czy możliwych do zastosowania środków technicznych i organizacyjnych mających na celu zabezpieczenie danych. Mogą być więc one pewnego rodzaju instrukcjami działania.

Idea tworzenia kodeksów postępowania (obecnie nazywanych kodeksami dobrych praktyk) nie jest nowa. W Polsce GIODO od dawna zachęcał do ich tworzenia i myślę, że to był dobry kierunek. Ogólne rozporządzenie o ochronie danych nadaje im jeszcze większą rangę, wskazując m.in., że muszą być zatwierdzone przez organy nadzorcze. **M.in. dzięki temu kodeksy, ze znanego dotąd narzędzia wizerunkowo-promocyjnego, staną się instrumentem o charakterze prawnym.** *Warto dodać, że ich* przestrzeganie będzie miało wpływ na wysokość administracyjnej kary pieniężnej nakładanej przez GIODO w przypadku naruszenia prawa.

Działań i inicjatyw GIODO mających na celu pomoc w dostosowaniu się do jak najlepszego wypełniania nowych obowiązków jest znacznie więcej. Dla przykładu wymienię jeszcze przygotowanie dwuczęściowego poradnika, jak rozumieć i stosować podejście oparte na ryzyku czy informację dotyczącą ważności zgód na przetwarzanie danych osobowych. To jedne z wyjaśnień, które były oczekiwane przez przedsiębiorców i zostały bardzo pozytywnie przyjęte. Działania te z pewnością będziemy kontynuować.

Oczekiwaniami firm, zwłaszcza małych i średnich, kierowaliśmy się też układając program konferencji organizowanej 29 stycznia 2018 r. w Warszawie z okazji XII Dnia Ochrony Danych Osobowych. Okazuje się bowiem, że takie zagadnienia, jak zastosowanie w praktyce profilowania czy zasady przejrzystości, wciąż wymagają przybliżenia.

Czy profilowanie jest rzeczywiście takim zagrożeniem? Przecież dla przedsiębiorców to duże ułatwienie i często oszczędności? Czy po 25 maja 2018 r. będą więc mogli korzystać z tego rozwiązania?

Ogólne rozporządzenie o ochronie danych (RODO) nie wprowadza zakazu profilowania. Nie zezwala natomiast, by na podstawie profilowania podejmować zautomatyzowane decyzje wywołujące skutki prawne lub istotnie wpływające na osobę, gdy brak jest innych niż zgoda przesłanek legalizujących tego typu działanie. Ważne i niezbędne jest też to, żeby w każdym przypadku, gdy prowadzone będzie profilowanie, niezależnie od jego skutku i wpływu, informować o takim fakcie osoby, których dane dotyczą. Myślę, że wiele nieporozumień związanych z możliwością wykorzystywania profilowania pod rządami RODO wynika z tego, że część osób nie bierze pod uwagę tego, że zgodnie z RODO, czym innym jest profilowanie, a czym innym podejmowanie decyzji opierającej się wyłącznie na zautomatyzowanym przetwarzaniu, np. profilowaniu. Wyjaśnieniu tych różnic i ich wpływie na możliwość dokonywania profilowania poświęcona będzie jedna z sesji organizowanej przez nas w Warszawie konferencji.

Podczas innych wydarzeń wchodzących w skład obchodów Dnia Ochrony Danych Osobowych jednym z ważniejszych tematów jest nowa rola administratora bezpieczeństwa informacji (ABI), a zgodnie z RODO inspektora ochrony danych. Co oprócz nawy się zmieni?

W Polsce jesteśmy w o tyle korzystnej sytuacji, że w 2015 r. te przepisy ustawy o ochronie danych osobowych, które odnoszą się do ABI, zostały rozbudowane i są zbliżone do rozwiązań zawartych w RODO. Niemniej przepisy rozporządzenia dotyczące inspektorów ochrony danych osobowych jeszcze bardziej wzmacniają pozycję tej osoby i dają jej więcej gwarancji niezależności. Rozszerzają też katalog zadań inspektora.

Jednym z nich jest doradzanie i informowanie w zakresie obowiązków, jakie na osoby przetwarzające dane i podejmujące decyzje nakładają przepisy prawa. Inspektor ma też nadzorować, czy obowiązki te są prawidłowo wykonywane, np. za pomocą sprawdzeń, audytów zgodności przetwarzania danych z przepisami RODO i wewnętrznymi regulacjami podmiotu, tzw. wewnętrznymi politykami.

Inspektor ochrony danych osobowych będzie miał także obowiązek współpracowania z organem nadzorczym, czyli z GIODO. W przepisach określono, że inspektor ma pełnić rolę punktu kontaktowego dla organu nadzorczego w każdym przypadku, gdy zajdzie taka potrzeba.

Obowiązkiem inspektora będzie również udzielanie pomocy osobom, których dane są przez zatrudniający go podmiot przetwarzane, tzn. objaśnianie im ich uprawnień i ułatwianie korzystania z nich, na przykład z uprawnienia dostępu do danych. Przepis rozporządzenia ogólnego stanowi, że każda osoba może kontaktować się z inspektorem ochrony danych we wszelkich sprawach, które dotyczą przetwarzania jej danych osobowych. Inspektor ochrony danych będzie więc swego rodzaju „tarczą" administratora danych.

Jednak trzeba podkreślić, że odpowiedzialność za przetwarzanie danych osobowych zgodnie z prawem cały czas będzie spoczywała na administratorze danych. Zatrudnienie inspektora nie zdejmuje z niego tej odpowiedzialności. Inspektor będzie wprawdzie przekazywał swoje uwagi, wytyczne czy wskazówki, ale to administrator, osoba zarządzająca będzie odpowiedzialna za ich wprowadzenie w życie.

Do istotnych zadań inspektora będą należały także wewnętrzne działania edukacyjno-szkoleniowe. Jeśli osoby kierujące daną firmą i jej pracownicy znają zasady i wymogi prawne

oraz rozumieją, czemu one mają służyć, zwykle starają się ich przestrzegać. Stąd rola inspektora w tym zakresie jest nie do przecenienia.

Jedną z ważniejszych różnic jest to, że obecne prawo umożliwia administratorowi danych powołanie ABI. Tymczasem RODO w wielu przypadkach wprowadza wymóg powołania inspektora. Dotyczy to podmiotów, których główna działalność polega na operacjach przetwarzania danych wymagających regularnego i systematycznego monitorowania osób, których dane są przetwarzane. Również organy administracji publicznej (z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości) muszą powołać IOD.

Co grozi tym administratorom, którzy w dniu rozpoczęcia stosowania rozporządzenia nie będą przygotowani do stosowania nowych przepisów?

Konsekwencjami przetwarzania danych osobowych niezgodnie z prawem mogą być, jak dotąd, kontrole i nakazy administracyjne, a już wkrótce będą nimi również kary finansowe nakładane przez GIODO. Rozporządzenie w sposób zharmonizowany wprowadza możliwość nakładania przez organy nadzorcze, czyli w Polsce GIODO, finansowych kar administracyjnych za nieprawidłowe przetwarzanie danych osobowych. Nie jest jednak dobrze, jeśli rozmowę o ochronie i systemie ochrony danych osobowych zaczyna się od kwestii kar. Idealnie byłoby, gdyby tych kar w ogóle nie było i żebyśmy nie musieli o nich mówić. I jeśli administratorzy będą rzeczywiście dobrze przygotowani, to tak będzie.

Dziękujemy za rozmowę.

Redakcja Infor.pl