

W sektorze publicznym - obowiązkowy inspektor

14.11.17

Od 25 maja 2018 r. na mocy RODO będziemy mieli inspektora ochrony danych, który zastąpi ABI-ego. Administratorzy sektora publicznego będą zobowiązani powołać takiego inspektora - mówi Paweł Makowski radca z Biura Generalnego Inspektora Ochrony Danych Osobowych.



**Rozmowa z Pawłem Makowskim
radcą z Biura GODO.**

- O co najczęściej pytają administratorzy danych z sektora publicznego? Jakie nowe obowiązki wynikają z rozporządzenia unijnego RODO dla instytucji rządowych i samorządowych?

- Można powiedzieć, że nowych obowiązków dla tych podmiotów nie będzie tak wiele. Ogólne rozporządzenie obejmuje podmioty sektora publicznego, ale wobec nich uregulowania przewidują kilka wyjątkowych sytuacji.

Mamy teraz na przykład administratora bezpieczeństwa informacji - ABI. Administrator może powołać takiego eksperta wewnątrz organizacji, w celu wsparcia w realizacji zadań wynikających z przepisów prawa ochrony danych. Od 25 maja 2018 r. na mocy RODO będziemy mieli inspektora ochrony danych, który zastąpi ABI-ego. Administratorzy danych z sektora publicznego będą mieli obowiązek, by go wyznaczyć.

Warto też wspomnieć o innej ważnej zmianie dotyczącej nowego uprawnienia Generalnego Inspektora Ochrony Danych Osobowych, jakim jest uprawnienie do nakładania administracyjnych kar pieniężnych, i propozycji Ministerstwa Cyfryzacji, by sektor publiczny wyłączyć spod tego typu sankcji. W przygotowanym przez ten resort projekcie ustawy o ochronie danych osobowych podmioty publiczne zostały bowiem potraktowane w szczególnie sposób, gdyż obniżono wyraźnie maksymalny wymiar kary, jaki będzie można zastosować wobec administratora danych z sektora publicznego z 20 mln euro do 100 tysięcy złotych. Na organy publiczne (np. ministerstwa) nie będzie zaś można nałożyć jakiegokolwiek kary.

- Generalny Inspektor wniósł uwagi do tego projektu ustawy, który powstał w Ministerstwie Cyfryzacji. Jakiego rodzaju są to zastrzeżenia?

-- Uwagi GODO do projektów ustaw przygotowanych w Ministerstwie Cyfryzacji liczą ponad 140 stron. Dotyczą m.in. rozluźniania nowych zasad ochrony danych osobowych i

obniżania przyjętych standardów w tym zakresie. Weźmy na przykład nasze zastrzeżenia do projektowanych przepisów w zakresie wspomnianych kar finansowych. Ideą administracyjnych kar pieniężnych, które wprowadza RODO jest to, by były odstraszające. Trudno uznać, by kwota 100 tys. zł spełniała taką rolę na przykład w przypadku ZUS, który przetwarza olbrzymie ilości danych o wielomilionowej wartości. Rozumiemy, że kara nie może utrudniać realizacji zadań publicznych, ale pamiętajmy, że 20 mln euro to jest maksymalny wymiar kary. A GIODO będzie miał 11 kryteriów, na podstawie których będzie oceniał, czy i w jakiej wysokości tę karę nałożyć.

- Nakładanie kar to przecież jedna pula pieniędzy publicznych!

- To prawda. Ale przecież Państwowa Inspekcja Pracy i sądy także decydują o nakładaniu różnego rodzaju sankcji finansowych na podmioty publiczne. I też można by przecież uznać, że to przenoszenie pieniędzy publicznych z kieszeni do kieszeni. Ale nie o to tutaj chodzi. Posłużę się bardzo interesującym przykładem szpitala w Chorzowie. W tym samym budynku mieszczą się i szpital publiczny, i niepubliczny. Wyobraźmy sobie sytuację, w której doszło do rażącego naruszenia prawa o ochronie danych; ujawniono dane medyczne pacjentów poprzez niewłaściwe zabezpieczenie dokumentacji. I my jako GIODO będziemy mogli szpital prywatny ukarać sankcją do 20 mln euro, a szpital publiczny za to samo naruszenie karą 100 tys. zł. Widzimy tutaj dużą dysproporcję.

Niemniej dyskusję rozpocząłbym od pytania, dlaczego mielibyśmy karać? Trzeba postępować zgodnie z prawem! Przecież podmioty publiczne muszą działać na podstawie i w granicach prawa. Ten, kto przestrzega prawa, nie będzie karany.

- Jakie inne uwagi zgłasza Pan do Ministerstwa Cyfryzacji w sprawie nowego projektu ustawy?

- Jednym z ważniejszych zastrzeżeń jest obniżenie standardu niezależności nowego organu chroniącego dane osobowe – obecnie GIODO. Kolejne dotyczą zmian w przepisach sektorowych. Mamy wrażenie, że poszły one za daleko, dalej niż przewiduje to art. 23 rozporządzenia (możliwe ograniczenia stosowania RODO). Mówię o sektorze bankowym, ubezpieczeniowym i statystyki publicznej. Rozporządzenie zawiera bardzo rozsądny balans między uprawnieniami administratorów danych a prawami osób, których dane dotyczą. Natomiast przepisy zaproponowane przez Ministerstwo Cyfryzacji faworyzują biznes. Na przykład sektor bankowy. Ostatnio były poważne wycieki z kilku banków w Polsce, a o tym poinformował niezależny portal. Na mocy rozporządzenia każdy taki wyciek powinien kończyć się informacją do Generalnego Inspektora i co ważniejsze - poinformowaniem klientów, jak mogą zabezpieczyć swoje dane, aby zapobiec ryzyku skradzenia ich tożsamości.

- W projekcie ustawy nie ma obowiązku takiej informacji?

- Okazuje się, że jeżeli taka informacja zagroziłaby stabilności sektora bankowego w Polsce, to nie będzie obowiązku informowania klientów o naruszeniu. Mamy, po jednej stronie bardzo ogólne pojęcie - stabilność sektora bankowego, a po drugiej stronie - prawo każdego obywatela do bycia poinformowanym. To stwarza duże ryzyko dla praw i wolności. Takie przepisy niszczą naturalną równowagę między administratorami danych a prawami obywateli. Na pewno nie będzie zgody GIODO na obniżanie standardów określonych w RODO.

- Wracając do sprawy niezależności nowego organu kontroli danych osobowych, którego zastępców mają wyznaczać ministrowie a nie ten organ. W czym upatruje Pan rozbieżności polskiej ustawy w stosunku do rozporządzenia unijnego?

- Rozporządzenie stanowi, że to państwa członkowskie decydują, kto powołuje organ. Może

to być parlament czy głowa państwa, zastrzega jednak, że trzeba zagwarantować pełną niezależność organu. A dorobek orzecniczy Trybunału Sprawiedliwości UE wyraźnie wskazuje, jak taką niezależność zapewnić (vide sprawa Komisja Europejska przeciwko Węgrom). W tym wyroku mówi się o „uprzednim posłuszeństwie” organu, wskazując, że nawet minimalny wpływ polityków na działalność organu tę niezależność przekreśla. A w polskiej ustawie mamy wybieralność przez polityków zastępców Inspektora, na co ten ostatni nie ma zupełnie wpływu. Prezes takiego organu - według rozporządzenia – powinien mieć natomiast pełną swobodę doboru swego personelu.

- Czy w ustawie polskiej zbyt szeroko nie potraktowano wyjątków od zasad przetwarzania danych i ich kontroli?

- GIODO zdecydowanie wyraża taką obawę, wskazując, że na podstawie art. 23 RODO istnieje możliwość ograniczenia stosowania przepisów tego rozporządzenia. Jednak każde takie ograniczenie musi być uzasadnione i przewidywać niezbędne gwarancje dla osób, których dane dotyczą. W projektowanych przepisach to uzasadnienie w wielu przypadkach bardzo ciężko znaleźć. Pamiętajmy jednak, że rozporządzenie ma bezpośrednie zastosowanie. Zatem zdecydowana większość praw i obowiązków wynika wprost z jego przepisów i będą one stosowane bezpośrednio, bez konieczności wprowadzania ich ustawą do polskiego porządku prawnego – jak np. obowiązki administratora czy prawa osób, których dane dotyczą.

- Jak wygląda wyłączenie związków wyznaniowych i kościołów?

- Tu sytuacja jest jednoznaczna. Jeśli kościoły i związki wyznaniowe nie mają innych przepisów, to stosuje się do nich RODO. Kościoły w różnych państwach pracują nad uregulowaniem swego statusu. Według naszej wiedzy, takie prace toczą się również w Polsce.

- Ministerstwo Cyfryzacji wprowadza jako nowość kodeksy postępowania.

- Prezes nowego urzędu będzie mógł je zatwierdzać i w krajowej ustawie należało wprowadzić przepisy proceduralne, czyli sposób funkcjonowania organu nadzorczego i wskazać jego kompetencje, wynikające z rozporządzenia. Ale to rozporządzenie, a nie polskie przepisy, wprowadzają kodeksy postępowania oraz mechanizmy ich opiniowania i zatwierdzania przez organ nadzorczy.

- Dlaczego to jest ważne?

- Dlatego, że wielu administratorów danych czeka na wejście w życie ustawy o ochronie danych, a przecież większość obowiązków, jak np. zasada rozliczalności, jak obowiązki informacyjne czy prawo do przenoszenia danych w odpowiednim formacie - wynika z RODO. Do spełnienia tych obowiązków trzeba się już przygotowywać, nie czekając na przepisy ustawy.

Rozmawiała: Katarzyna Żaczkiewicz-Zborska

[Katarzyna Żaczkiewicz-Zborska](#) 14.11.17