

# Urząd GIODO musi być silny i niezależny

W: Przedstawiony przez Ministerstwo Cyfryzacji Projekt ustawy o ochronie danych osobowych zakłada zastąpienie generalnego inspektora przez prezesa urzędu ochrony danych osobowych (UODO). Jak się Pani odnosi się do tego pomysłu?

DR EDYTA BIELAK-JOMAA, GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH: Trudno się do tego odnosić, bo nie wiem, co oznacza sformułowanie „nowy urząd”. Nie ma w projektowanej ustawie przepisów ustrojowych dotyczących jego utworzenia. Nie wyobrażam sobie, że powołany zostanie zupełnie nowy organ, a obecny będzie zlikwidowany. GIODO jest organem od dwudziestu lat stojącym na straży podstawowych praw człowieka, jakimi są prawo do ochrony danych osobowych i prawo do prywatności. Te 20 lat działalności to ogromna wiedza, długoletnia praktyka, długotrwała współpraca z innymi organami ochrony danych osobowych w Europie i na świecie, zaangażowanie w prace nad reformą ochrony danych oraz wdrożeniem rozporządzenia na polu krajowym i europejskim. Nowych rozwiązań nie można tworzyć w oderwaniu od wiedzy i doświadczenia GIODO. Dlatego przedstawiony przez Ministerstwo Cyfryzacji projekt, zwłaszcza że jest szcztąkowy, traktuję jako otwarcie dyskusji. Już najwyższy czas, żeby się rozpoczęła.

**Projekt zakłada przede wszystkim, że kontrole mają trwać krócej. GIODO dostanie też więcej obowiązków w związku z samym rozporządzeniem. Czy potrzebne będą dodatkowe zasoby kadrowe i finansowe, aby podjąć tym zadaniom?**

GIODO musi być organem silnym i niezależnym, bo tylko taki jest w stanie skutecznie i efektywnie wypełniać nałożone na niego zadania. Niezależny i silny organ to taki, który ma zapewnione odpowiednie środki organizacyjne, finansowe i kadrowe. Czekamy aż Ministerstwo Cyfryzacji przedstawi tę część projektu ustawy, która określi te kwestie. Są one kluczowe dla dalszego, skutecznego działania. Wiedza w tym zakresie jest niezbędna, by właściwie planować przyszłoroczny budżet, a także po to, by pisać sprawozdanie z rocznej działalności GIODO, móc odpowiednio sformułować plany na przyszłość.

**Czy jest już jakaś koncepcja jak wymagania ws. certyfikacji będą wyglądać?**

Mechanizmy certyfikacyjne zostały kompleksowo uregulowane przez ustawodawcę unijnego. W pewnym zakresie zostaną jeszcze uzupełnione przez Komisję Europejską. Natomiast na poziomie krajowym przede wszystkim należy odpowiedzieć na pytanie, kto ma nadawać certyfikaty akredytować podmioty certyfikujące. Ogólne rozporządzenie przewiduje, że certyfikaty mogą być nadawane przez akredytowane podmioty certyfikujące lub organy ochrony danych osobowych.

W naszej ocenie, krąg tych podmiotów powinien być jak najszerszy, czyli obejmować także GIODO. Niestety, Ministerstwo Cyfryzacji nie przewiduje takiej kompetencji dla organu ochrony danych osobowych. W różnych państwach europejskich to właśnie organy ochrony danych osobowych prowadzą programy certyfikacyjne, co w żaden sposób nie ogranicza innych podmiotów certyfikujących, lecz raczej ten rynek wzmacnia i stymuluje.



Tym bardziej, że teraz już nie będziemy mogli mówić o jedynie o krajowym rynku certyfikatów lecz o rynku europejskim i to tam będzie się rozgrywała konkurencja pomiędzy dostępnymi mechanizmami certyfikacyjnymi.

**Ostatnio GIODO zawarł kilka porozumień dotyczących samoregulacji, choćby ze związkiem pracodawców branży Internetowej (IAB Polska). Czy zamierzacie Państwo rozwijać ten trend?**

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. Również ogólne rozporządzenie o ochronie danych przewiduje tworzenie takich dokumentów przez zrzeszenia i inne podmioty reprezentujące określone kategorie administratorów lub podmioty przetwarzające. Nowością jest jednak to, że kodeksy muszą być zatwierdzone przez organy nadzorcze. Uważam, że ich opracowywanie przyczyni się do upowszechnienia wiedzy związanej z nowymi zasadami przetwarzania danych określonymi w rozporządzeniu. Ponadto jest to dobry sposób zaangażowania samych administratorów w proces wdrażania nowych przepisów. Warto dodać, że przestrzeganie takich kodeksów będzie miało wpływ na wysokość kary admi-nistracyjnych nakładanych przez GIODO, ale nie wyłącza w żadnym aspekcie możliwości kontrolnych organu ochrony danych.

**Dla podmiotów publicznych kary nie mogą przekraczać 100 tys. zł. Będą one odczuwalne i spełnią funkcję odstraszającą?**

Rozważając kwestię wysokości kar powinniśmy przede wszystkim mówić o równości podmiotów. Jaka jest różnica między szpitalem publicznym a prywatnym, w sytuacji gdy doszło w nich do wycieku danych osobowych pacjentów? Z perspektywy osób, których dane zostały utracone, sytuacja jest taka sama. I jeden, i drugi

podmiot utracił władztwo nad danymi, a pacjenci ponieśli taką samą szkodę. Dodatkowo warto zaznaczyć, że do tej pory w sektorze publicznym poziom zgodności z przepisami o ochronie danych osobowych zazwyczaj był wyższy niż w sektorze prywatnym. Czy tak będzie dalej – nie wiadomo. Mamy świadomość, że kara za niezgodne z prawem przetwarzanie danych osobowych płaconą przez podmiot publiczny to przekładanie pieniędzy z jednej publicznej kieszeni do drugiej. Dlatego jeśli mielibyśmy obniżyć kary finansowe w tym sektorze, to trzeba by zastosować inne narzędzia, które będą mobilizowały do dbałości o dane osobowe. Obecnie nie wiemy np., co będzie z odpowiedzialnością karną, bo Ministerstwo Cyfryzacji nie zaproponowało żadnych przepisów w tym zakresie.

Z perspektywy GIODO ważne jest, żeby wszystkie podmioty przestrzegały prawa. Nie chcemy w pierwszej kolejności mówić o karach, tylko o tym, jak prawidłowo stosować przepisy. Cały czas o to zabiegamy, m.in. poprzez organizację i udział w seminariach i konferencjach, organizację szkoleń dla ABI – przyszłych inspektorów ochrony danych czy opracowywanie i publikację materiałów edukacyjno-informacyjnych. Działania te kierujemy do wszystkich administratorów – publicznych i prywatnych. Chcemy, żeby GIODO był organem efektywnym i mogącym elastycznie reagować na kwestie związane z przetwarzaniem danych, również po 25 maja 2018 r. Stąd też nasze propozycje kierowane do Ministerstwa.

**Jakie to propozycje?**

Z ogromną satysfakcją odnotowaliśmy to, że nasz pomysł na jednoinstancyjne postępowanie został przyjęty w projekcie Ministerstwa Cyfryzacji. To z pewnością doprowadzi do zwiększenia szybkości postępowania i poprawy jego efektywności. Mimo iż GIODO jako niezależny organ, usytuowany poza Radą Ministrów, nie ma inicjatywy

ustawodawczej, to w miarę możliwości kadrowych – wspiera rząd i poszczególne resorty w prowadzonych pracach. Prowadzi też własne prace przygotowawcze. Jednym efektów było opracowanie i przekazanie do resortu cyfryzacji projektu procedury postępowania przed GIODO. Niestety, nasz pomysł został okrojony i zmodyfikowany w sposób, który może prowadzić do osiągnięcia przeciwnego efektu.

**Czy rozporządzenie wzmocni współpracę na szczeblu europejskim i pozwoli lepiej kontrolować przetwarzanie danych przez podmioty międzynarodowe?**

Samo uchwalenie rozporządzenia sprawia, że ochrona jest przeniesiona na poziom międzynarodowy. Jest to akt prawny, który bezpośrednio obowiązuje w każdym państwie członkowskim UE w tym samym zakresie. GIODO będzie członkiem Europejskiej Rady Ochrony Danych (EROD), składającej się z rzeczników ochrony danych państw europejskich, która będzie miała swoje kompetencje, m. in. do rozstrzygania sporów pomiędzy organami przy wydawaniu decyzji, gdy sprawa będzie prowadzona przez tzw. organ wiodący, przy udziale organu innego państwa. EROD będzie miała niezwykle istotne znaczenie także przy certyfikacji czy przekazywaniu danych do państw trzecich, które nie gwarantują odpowiedniego poziomu ich ochrony. Zniknie natomiast ciało doradcze w postaci Grupy Roboczej Artykułu 29.

**Jak wyobraża sobie Pani relację między UODO, a inspektorami ochrony danych, którzy zgodnie z rozporządzeniem będą musieli być powołani w każdej instytucji?**

Według rozporządzenia, inspektorem ochrony danych ma być osoba o odpowiedniej wiedzy i z jednej strony wspierająca administratora danych w zgodnym z prawem ich przetwarzaniu, z drugiej zaś – niejako monitorująca jego zadania. Dlatego inspektor ma podlegać bezpośrednio administratorowi danych. Dzięki temu w każdej chwili, jeśli działania administratora, czyli konkretnie dyrektora, prezesa czy ministra, będą niezgodne z prawem, może do niego pójść i powiedzieć: „Stop! Tego robić nie powinienś, bo grozi ci odpowiedzialność finansowa”. Albo: „Nie mamy polityki w zakresie bezpieczeństwa danych osobowych i powinniśmy ją stworzyć”.

Taki inspektor powinien być też w każdym czasie dopuszczony do informacji o tym, jakie dane są przetwarzane i dlaczego, by miał wiedzę, co się dzieje w tym zakresie u administratora i mógł podpowiadać mu, ale też zwracać uwagę na naruszenia i nie dopuszczać do nich. Inspektor ochrony danych ma być też punktem kontaktowym dla osób, których dane są przetwarzane. Postrzegamy ich więc jako wsparcie – nie urzędu, bo często są mylnie uważani za „piątą kolumnę” GIODO w strukturach administratora – ale systemu ochrony danych osobowych danej instytucji. To administrator będzie odpowiedzialny za przetwarzanie danych i w jego interesie będzie mieć dobrego inspektora ochrony danych. GIODO chce pomóc w budowie takiego systemu i dlatego w tej chwili jednym z naszych priorytetów jest wspieranie kształcenia inspektorów ochrony danych, zarówno poprzez organizację dedykowanych im sektorowych szkoleń, jak i poprzez utworzenie specjalnego serwisu informacyjnego na stronie internetowej. ©

–rozmawiał Szymon Cydzik