

Potraktujmy RODO jako wyzwanie

Z Generalnym Inspektorem Ochrony Danych Osobowych Edytą Bielak-Jomaa, doktor nauk prawnych, rozmawia Dorota Bąbiak-Kowalska.

Spotykamy się na 160 dni przed rozpoczęciem stosowania unijnego ogólnego rozporządzenia o ochronie danych osobowych (RODO lub rozporządzenie). Z rozmów z samorządowcami wynika, że świadomość RODO w jednostkach samorządowych jest na ogół dość wysoka, ale jeśli chodzi o fizyczne przygotowanie się do stosowania tych przepisów, to samorządy mają jeszcze bardzo dużo do zrobienia. Na jakim etapie są przygotowania jednostek samorządowych?

Bardzo mnie cieszy, że samorządowcy twierdzą, iż wiedzą o zbliżających się zmianach w prawie i są na nie przygotowani. Natomiast jak jest faktycznie, okazało się po 25 maja 2018 r. To jest wyzwanie dla nas wszystkich: dla administratorów danych, organów ochrony danych osobowych oraz dla krajowego ustawodawcy.

Niemniej jednak chciałabym podkreślić, że podstawą tej reformy są dwa akty prawne na poziomie europejskim: tak zwane ogólne rozporządzenie o ochronie danych osobowych i tak zwana dyrektywa policyjna (choć ta nazwa jest myląca, bo dyrektywa nie dotyczy tylko policji, czyli spraw związanych z dochodzeniem i wykrywaniem przestępstw, ale również wymiaru sprawiedliwości). Dla nas zasadnicze znaczenie ma ogólne rozporządzenie, gdyż jest to akt, który bezpośrednio obowiązuje we wszystkich państwach Unii Europejskiej, regu-

lując prawa obywateli i obowiązki administratorów danych. Harmonizuje on porządku prawne wszystkich państw należących do Unii Europejskiej, a jego celem jest podniesienie poziomu ochrony danych osobowych tak, aby był on maksymalnie wysoki. Żeby obywatele mieli poczucie, że ich prywatność jest szanowana, a ich dane osobowe są przetwarzane zgodnie z prawem. Z drugiej strony rozporządzenie ma ułatwić swobodny przepływ danych osobowych w ramach Unii Europejskiej, żeby gospodarka mogła się rozwijać.

Niezwykle istotne, co trzeba podkreślać, jest to, że administratorzy danych już teraz powinni prowadzić intensywne prace związane z wdrożeniem nowych rozwiązań, nie czekając na jakiegokolwiek 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 zrab reformy, to on jest już gotowy i już trzeba przygotowywać się do stosowania nowych regulacji. Podsumowując, cieszy mnie świadomość sa-



To szef będzie ponosił odpowiedzialność za cały system ochrony danych w danym podmiocie. I to od niego będzie zależało, jak ta ochrona będzie wyglądać.

morządowców co do zmian w systemie ochrony danych osobowych, natomiast to, jak one będą wdrożone w praktyce, będę umiała powiedzieć, gdy już zaczniemy stosować te nowe przepisy.

W jaki sposób te zmiany wpłyną na mieszkańców, którzy występują w roli klientów JST? Czy mogą się oni czuć bezpiecznie?

Kontynuując myśl z poprzedniej odpowiedzi: jeśli samorządy są dobrze przygotowane do stosowania nowych regulacji, to mieszkańcy mogą się czuć bezpiecznie.

Oczywiście nie jesteśmy w stanie zagwarantować, że nigdy nic się nie wydarzy, nie nastąpi utrata danych albo nieprawidłowy proces ich przetwarzania, ktoś zastosuje nieodpowiednie narzędzia techniczne. Z góry nie możemy niczego zakładać. Wiemy, że mamy przepisy prawa, które będą stosować ludzie, a to człowiek jest zawsze zarówno tym najsilniejszym, jak i najsłabszym ogniwem.

Natomiast rozporządzenie wprowadza wiele nowych rozwiązań, które wzmacniają prawa obywateli, a więc m.in. klientów samorządów, i mają zwiększyć poziom ochrony ich danych. Jeśli mówimy o prawach obywateli, to w przepisach prawa najczęściej temu prawu odpowiada bezpośrednio obowiązek administratora danych. Jeśli obywatel ma mieć prawo do tego, aby być poinformowanym o tym, jakie jego dane są gromadzone, przez kogo, na jakiej podstawie prawnej, w jakim celu, komu będą udostępniane, jak długo będą przechowywane, to temu prawu obywatela odpowiada obowiązek administratora do przekazywania takiej informacji już w chwili pozyskiwania danych. Administrator, co jest niezwykle istotne, zgodnie z przepisami RODO, ma obowiązek informować obywatela w taki sposób, aby przekazywana informacja była jasna, klarowna, czytelna, aby jego komunikat był zrozumiały, a każdy odbiorca tej informacji wiedział, dlaczego jego prywatność ma być naruszona i w jakim zakresie.

W jaki sposób wójt, burmistrz, prezydent może sprawdzić, czy jego urząd jest gotowy na RODO? Ma, założymy, powołany zespół ekspertów odpowiedzialnych za wdrożenie tych prze-

pisów, ale skąd ma mieć pewność, że wszystko przebiega jak należy i urząd jest gotowy na 25 maja 2018 r.?

To jest właśnie jądro problemu. Niektórzy mówią, że reforma systemu ochrony danych osobowych to rewolucja, a my mówimy, że to jest zmiana podejścia do ochrony danych osobowych. Przenosi się ciężar odpowiedzialności za procesy przetwarzania danych osobowych na ich administratorów. To szef będzie ponosił odpowiedzialność za cały system ochrony danych w danym podmiocie. I to od niego będzie zależało, jak ta ochrona będzie wyglądać. Na nim zatem spoczywa obowiązek zapewnienia, aby osoby, które przetwarzają dane, miały odpowiednią wiedzę, kompetencje, umiejętności. Jeżeli dopuszcza pracowników do przetwarzania danych osobowych, to musi im nadać upoważnienia do przetwarzania danych. Trzeba dokonać podziału ról pomiędzy pracowników i dostosować do tej organizacji zabezpieczenia techniczne. I to też nie będzie zapewne łatwe, bo to administrator danych będzie musiał ocenić, jakie dane przetwarza, jakie jest ryzyko związane z przetwarzaniem tych danych. Zupełnie inne jest ryzyko, jeśli przetwarza się niewiele rekordów, które zawierają imię, nazwisko i adres zamieszkania, a inne, jeśli przetwarza się dane wrażliwe, np. o sytuacji rodzinnej, wyznaniu, wyrokach, sytuacji materialnej, zdrowiu, nałogach itp. Utrata takich danych naraża na ryzyko utraty wiarygodności, wkroczenie w sferę prywatności czy intymności, być może także na kradzież tożsamości. Im większe jest ryzyko wkroczenia w sferę prywatności, tym lepsze zabezpieczenia organizacyjne i techniczne trzeba wprowadzić. I ten obowiązek, ta odpowiedzialność spoczywa na administratorze danych.

Pomocą dla niego z całą pewnością będzie inspektor ochrony danych, czyli taka osoba, która dzisiaj nazywana jest administratorem bezpieczeństwa informacji (ABI). To ekspert, którego wiedza, doświadczenie i umiejętności to fundament, na którym zbudować można system skutecznej ochrony danych osobowych danego podmiotu. Żeby tak się stało, niezwykle istotne jest umiejscowienie takiej osoby w strukturze organizacyjnej jednostki i zapewnienie mu niezależno-

ści w działaniu, do czego zresztą RODO wprost zobowiązuje. Pamiętać również należy, że – zgodnie z RODO – wszystkie organy i podmioty publiczne będą zobowiązane do wyznaczenia takiego inspektora ochrony danych.

Co grozi tym samorządom, które w dniu wejścia w życie rozporządzenia nie będą przygotowane 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 na administratorów danych 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 tym mówić. I jeśli administratorzy, w tym samorządy, będą rzeczywiście dobrze przygotowani, to tak będzie.

Natomiast one są przewidziane i trzeba o tym wspomnieć. Rozporządzenie wprowadza górną ich granicę – jest to 20 mln euro bądź do 4 proc. rocznego światowego obrotu. Ale umówmy się, chodzi tutaj z całą pewnością o wielkich graczy, dla których 20 mln euro to nie są wielkie pieniądze. Natomiast jeśli chodzi o administrację publiczną i podmioty publiczne, to ze strony Ministerstwa Cyfryzacji (odpowiedzialnego za dostosowanie polskich przepisów do postanowień RODO) mamy propozycję, aby w nowej ustawie o ochronie danych osobowych wprowadzić przepis przewidujący, że kary, które będą mogły być nakładane na administrację i podmioty publiczne, nie były wyższe niż 100 tys. złotych. My, jako organ ochrony danych osobowych, takie rozwiązanie podajemy jednak analizie krytycznej. Budzi ono bowiem wątpliwości z punktu widzenia równości podmiotów prawa, a także z punktu widzenia obywateli. Proszę bowiem wyobrazić sobie i odpowiedzieć na pytanie, czym różni się sytuacja przeciętnego Kowalskiego, gdy np. w szpitalu prywatnym giną lub

są sprzedane informacje z jego karty chorobowej, czyli dane najbardziej wrażliwe, i taki szpital będący szpitalem niepublicznym jest obciążony odpowiedzialnością do 20 mln euro, od sytuacji, gdy ze znajdującego się czasem w tym samym budynku albo w tym samym mieście szpitala publicznego następuje dokładnie taki sam wyciek, może nawet dotyczący tego samego Kowalskiego, i ten podmiot będzie mógł ponieść karę za to samo przewinienie 400-krotnie niższą. Z perspektywy Kowalskiego szkoda jest taka sama, a podmioty będą mogły ponosić różną odpowiedzialność. Z tego powodu krytykujemy takie zróżnicowanie. Wszyscy musimy czuć reżim prawidłowego stosowania przepisów i odpowiedzialność. Wówczas kary nie będą musiały być nakładane.

Nie lubię mówić o karach, bo to też nie jest tak, że chodzi tylko o pieniądze. Istotne jest bowiem budowanie zaufania między obywatelem a np. samorządem. Chciałabym mieć poczucie, że ktoś, kto wykorzystuje moje dane osobowe, rzeczywiście odpowiedzialnie obchodzi się z informacjami na mój temat i że są one bezpieczne. A w samorządach tych informacji, często wrażliwych, jest bardzo dużo, bo dla różnych celów są gromadzone.

Gdzie samorządy mogą szukać pomocy, wskazówek, jak przygotować się do wejścia w życie tych przepisów? Rynek został zalany ofertą podmiotów oferujących różnego rodzaju szkolenia i kursy przygotowujące do ich wdrożenia. Jak poruszać się w gąszczu tych ofert?

Ważne są dwie rzeczy. Po pierwsze, trzeba zacząć działać, zwłaszcza jeśli ktoś nie jest jeszcze w ogóle przygotowany do stosowania rozporządzenia. Co zrobić? 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. Dla sprawdzenia stanu przygotowania można też zadać sobie np. pytanie, czy wiem, jak postąpić, gdyby ktoś przyszedł dziś i zażądał usunięcia danych, które są przetwarzane. Kto wówczas wydaje decyzje w tej sprawie? Jak przebiega ta procedura?

Po drugie, wiemy, że do samorządów są kierowane różne oferty, w których straszy się ich GIODO i karami. Uczulam, aby wszyscy administratorzy dokonywali wyboru takich ofert w odpowiedzialny i rozważny sposób. Sami powinni wiedzieć, jakiego wsparcia potrzebują, jaką wiedzę chcieliby zdobyć podczas szkoleń czy warsztatów. Zachęcam do korzystania z bogatej oferty w tym zakresie, ale także do porządnej weryfikacji firm, które te szkolenia i pomoc proponują.



Administrator, co jest niezwykle istotne, zgodnie z przepisami RODO ma obowiązek informować obywatela w taki sposób, aby przekazywana informacja była jasna, klarowna, czytelna, aby jego komunikat był zrozumiały, a każdy odbiorca tej informacji wiedział, dlaczego jego prywatność ma być naruszona i w jakim zakresie.

Poza tym zapraszam do odwiedzania strony internetowej Generalnego Inspektora Ochrony Danych Osobowych – www.giodo.gov.pl. Jednym z udostępnionych na niej materiałów jest poradnik „Czy jesteś gotowy na RODO”. Krok po kroku, w bardzo przystępnej formie, przedstawiono w nim, co powinni zrobić, o czym powinni pamiętać administratorzy danych, aby spokojnie oczekiwać 25 maja 2018 r.

Zachęcam również, aby na bieżąco śledzić zakładkę „Reforma przepisów”, na której na bieżąco staramy się umieszczać wiele różnych materiałów

przydatnych do przygotowania się do stosowania RODO, takich jak np. wytyczne Grupy Roboczej Art. 29. Nie oszukujmy się, rozporządzenie nie jest łatwe, stąd też europejskie organy ochrony danych korzystają z prawa dawania wskazówek, jak rozumieć i w praktyce stosować jego przepisy. Ponadto aktywnie wspieramy administratorów danych w przygotowaniach do RODO poprzez wspieranie administratorów bezpieczeństwa informacji, czyli przyszłych inspektorów ochrony danych. W ostatnim czasie organizujemy dla nich specjalne, sektorowe szkolenia. Wzięło w nich udział już około 1,5 tysiąca ABI z takich sektorów, jak szkoły wyższe, sądy czy ośrodki oraz domy pomocy społecznej. Działania te będziemy kontynuować również w 2018 roku. Udało nam się pozyskać unijne dofinansowanie na szkolenia dla inspektorów ochrony danych z sektora publicznego – tzw. projekt T4DATA zakłada przeszkolenie grupy 600 inspektorów.

Z samorządowcami spotykamy się ponadto przy różnych okazjach: konferencjach, spotkaniach w urzędach miast czy w mniejszych miejscowościach. Staramy się być, rozmawiać o reformie i gdy są problemy podpowiadać rozwiązania. Ale też uczulamy, że te wyzwania, które stoją przed samorządami, to jest poważna sprawa. I że zgodnie z RODO trzeba do niej poważnie, ale i samodzielnie podejść.

Jakie największe zagrożenie widzi pani przed 25 maja 2018 r.? Z czym samorządy mogą mieć największy problem? I czy jest jakiś plan B, plan naprawczy dla tych, którzy nie zdążą z przygotowaniem do RODO?

Nie mam wątpliwości, że nie będzie tak, iż 25 maja 2018 r. wszyscy będą mówić „mamy absolutnie w 100 proc. gotowy urząd na obowiązywanie nowych przepisów”. Natomiast chcę wierzyć w to, że jeśli odpowiedzialnie administratorzy mówią „jesteśmy przygotowani, wiemy czego się spodziewać, wiemy co robić”, nie będzie potrzebny żaden plan B. Wiedząc, że to nie pierwsze tak ogromne wyzwanie dla samorządów, ufam, że dadzą radę. I że to nie grożące kary finansowe ich do tego zmotywują, ale chęć ochrony danych osobowych mieszkańców, troska o prawidłowe, zgodne z prawem ich przetwarzanie. ■