

ZM!ANY 2018

Od 2018 roku rewolucyjne zmiany przepisów w zakresie ochrony danych osobowych

W życie weszło rozporządzenie Parlamentu Europejskiego w sprawie ochrony danych osobowych. Jego rozwiązania będą stosowane w Polsce za niecałe dwa lata. Będzie to rewolucja – obywatele zyskają nowe narzędzia ochrony zaś na administrację publiczną nałożone zostaną nowe obowiązki.

Czy rozporządzenie PE i Rady UE z kwietnia 2016 r. w istotny sposób zmieni sposób postępowania administratorów danych? Jakie narzędzia zyska GIODO, by chronić nas przed nieuczciwymi praktykami z ich strony?

– Rozporządzenie wprowadza wiele nowych rozwiązań, jak np. prawo do bycia zapomnianym czy prawo do przenoszenia danych. Ustanawia też nowy sposób dopełniania obowiązku informacyjnego, a także obowiązek prowadzenia rejestru czynności (operacji) przetwarzania danych osobowych. Ponadto, wprowadzając generalną zasadę uwzględniania zasad ochrony danych już w fazie projektowania procesów przetwarzania danych osobowych, przenosi ciężar odpowiedzialności za niezgodne z prawem przetwarzanie danych osobowych na administratorów danych.

Z kolei GIODO, gdy dane osobowe będą przetwarzane niezgodnie z przepisami, będzie miał prawo nakładania administracyjnych kar pieniężnych. Z samego założenia mają one być skuteczne, proporcjonalne i odstrasżające. W mojej ocenie, świadomość, że można zapłacić bardzo wysoką karę za niewłaściwe przetwarzanie danych, będzie mobilizowała do większej dbałości o nie.

Zgodnie z rozporządzeniem, skargi będą mogły być składane do krajowych inspektorów, bez względu na siedzibę firmy, która jest skarżona. Jakie narzędzia będzie posiadał GIODO, by wyegzekwować ochronę polskich obywateli? Jak będzie wyglądała zacieśniona współpraca między GIODO i analogicznymi instytucjami w innych krajach UE?

– Rozporządzenie – dzięki temu, że będzie stosowane bezpośrednio, bez konieczności implementacji do



Z dr Edytą Bielak-Jomaa,
Generalnym Inspektorem
Ochrony Danych Osobowych
(GIODO)
rozmawia Rafał Osiński

krajowych porządków prawnych – doprowadzi do unifikacji zasad ochrony danych osobowych we wszystkich państwach UE. Ułatwieniem będzie możliwość składania skargi bezpośrednio do krajowego organu ds. ochrony danych osobowych – w Polsce do GIODO. Rozporządzenie stanowi zaś, że nasza instytucja będzie przekazywała ją do organu ochrony danych tego kraju UE, w którym znajduje się główna jednostka organizacyjna administratora lub podmiotu przetwarzającego. Zagraniczny organ będzie miał obowiązek współpracować z nami w zakresie rozpatrywania skargi. Z kolei GIODO, w ramach uprawnień, oprócz prawa do otrzymywania informacji i wydawania opinii dotyczących projektu decyzji, będzie miał również kompetencje do kształtowania jej treści. Jeżeli bowiem projekt decyzji byłby niezadowolający, Generalny Inspektor będzie uprawniony do złożenia sprzeciwu.

Ponadto, w wyjątkowych okolicznościach, jeżeli GIODO uzna, że istnieje pilna potrzeba podjęcia działań w celu ochrony praw i wolności osób, których dane dotyczą, będzie mógł przyjąć środki tymczasowe, które

na terenie Polski wywołają skutki prawne przez określony czas.

Jeśli zaś chodzi o współpracę unijnych organów ds. ochrony danych osobowych, to będą one zobowiązane do przekazywania sobie informacji i świadczenia wzajemnej pomocy. Ponadto rozporządzenie daje im możliwość prowadzenia wspólnych operacji (np. postępowań i egzekucji).

Jakie narzędzia ochrony zyskają polscy i unijni obywatele dzięki rozporządzeniu?

– W tym względzie warto wskazać na dwa mechanizmy mające na celu zwiększenie ochrony naszej prywatności – *privacy by design* (prywatność w fazie projektowania), zakładający, że narzędzia i usługi powinny być tak konstruowane, by od samego początku uwzględniały potrzebę ochrony prywatności obywateli, oraz *privacy by default* (prywatność w ustawieniach domyślnych). Mechanizm ten wskazuje, iż podstawowe ustawienia powinny chronić prywatność użytkownika, gromadzić minimalny zakres danych osobowych i dawać mu swobodę decydowania w tym zakresie.

Rozwinięciem praktycznych aspektów ochrony prywatności w fazie projektowania jest zaś dokonywanie oceny ryzyka i skutków wpływu projektu na prywatność oraz poziom ochrony danych (*privacy impact assessment*). Do jej przeprowadzania administrator danych lub podmiot przetwarzający są zobowiązani wówczas, gdy operacje przetwarzania stwarzają szczególne ryzyko dla praw i wolności podmiotów danych z racji swego charakteru, zakresu lub celów. Żeby przynosiła ona oczekiwane rezultaty, powinna być przeprowadzana jeszcze zanim jakieś urządzenia czy systemy zostaną wprowadzone do użycia. Duże znaczenie może też mieć przyjęcie koncepcji *risk based approach*, która zakłada, że im większe jest ryzyko związane z przetwarzaniem danych osobowych, tym większy powinien być zakres obowiązków ciążących na administratorze. W tym kontekście do zwiększonej dbałości o dane osobowe będą zobowiązani administratorzy korzystający z takich rozwiązań technologicznych, jak np. Big Data czy chmura obliczeniowa (*cloud computing*). O wymogu przywiązywania szczególnej wagi do zabezpieczenia danych decydowała będzie również sama treść gromadzonych informacji. Im zakres przetwarzanych danych jest szerszy bądź znajdują się w nim dane osobowe wrażliwe, tym poziom zabezpieczenia danych powinien być wyższy.

Jakie są plany kontroli GIODO w najbliższym czasie w sferze samorządu terytorialnego? Z czego wynikają takie plany?

– W planie kontroli sektorowych GIODO na 2016 rok znalazło się m.in. przeprowadzenie kontroli w starostwach powiatowych w zakresie przetwarzania danych osobowych w ewidencji gruntów i budynków. Kontrole takie odbyły się w 10 jednostkach, ale obecnie postępowania wszczęte na ich skutek są jeszcze w toku.

W tym roku planujemy też skorzystać z narzędzia, jakim są sprawdzenia dla GIODO, o których mowa w art. 19b ustawy o ochronie danych osobowych. Są one przeprowadzane przez administratorów bezpieczeństwa informacji (ABI) na wniosek GIODO. W tegorocznym harmonogramie takich sektorowych sprawdzeń przewidziane jest zbadanie realizacji przez gminy obowiązków informacyjnych wskazanych w art. 24 i art. 33 ustawy o ochronie danych osobowych.

Trzeba jednak zaznaczyć, że GIODO może też inicjować kontrole doraźne. W ostatnim okresie impulsem do rozpoczęcia takiej kontroli w jednostce samorządu terytorialnego stały się publikacje prasowe dotyczące upublicznienia na stronie internetowej urzędu miasta odpowiedzi na interpelację radnych, która zawierała imiona i nazwiska, numery PESEL, adresy oraz zarobki stażystów Miejskiego Ośrodka Pomocy Społecznej.

Jak samorząd terytorialny radzi sobie z przestrzeganiem przepisów o ochronie danych osobowych? Czy postępująca informatyzacja sprzyja ochronie?

– W mojej ocenie jest lepiej niż było i warto pochwalić urzędników za chęć pogłębiania wiedzy na temat ochrony danych osobowych, co potwierdza m.in. coraz częstsze i liczniejsze ich uczestnictwo w szkoleniach organizowanych przez GIODO. Niemniej nie osiągnęliśmy jeszcze stanu, który mógłby w pełni zadowalać. Częściowo jest to spowodowane tym, że kwestie przetwarzania danych osobowych w jednostkach samorządu reguluje wiele przepisów szczególnych, a ich interpretacja i właściwe zastosowanie przysparza niekiedy problemów.

Jeśli zaś chodzi o informatyzację urzędów, to z pewnością jest to proces nieuchronny, stanowiący jednocześnie duże wyzwanie: z jednej strony pomaga w codziennym życiu, zarówno petentom, jak i urzędnikom, z drugiej zaś – powoduje także zagrożenia w dziedzinie ochrony danych osobowych i prywatności.

Jakie problemy związane z ochroną danych osobowych rodzi program 500+? Czy zgłaszane wcześniej przez GIODO wątpliwości zostały przez ustawodawcę wyjaśnione?

– Na etapie prac legislacyjnych nad projektem ustawy o pomocy państwa w wychowywaniu dzieci, GIODO zgłaszał zastrzeżenia, wskazując m.in., że przyjmowane rozwiązania, zwłaszcza odnoszące się do zmian dotyczących administratora danych oraz instytucji powierzenia przetwarzania danych, będą rodziły wątpliwości interpretacyjne i mogą spowodować trudności w praktycznym stosowaniu przepisów. Uwagi te nie zostały jednak uwzględnione.

W związku z tym GIODO, dążąc do wsparcia administratorów danych przy realizacji programu i do zapewnienia poszanowania praw osób, których dane są przetwarzane, wydał komunikat mający na celu wyjaśnienie wątpliwości interpretacyjnych i przedstawienie stanowiska organu w tej sprawie.

Kolejny z komunikatów odnosił się do wątpliwości, jakie pojawiły się w kwestii zgłaszania do rejestracji GIODO zbiorów danych tworzonych w związku z realizacją Programu Rodzina 500+. Zawarte w nim wyjaśnienia stanowiły istotne wsparcie dla podmiotów zaangażowanych w realizację Programu.

Ponadto GIODO udzielał indywidualnych wyjaśnień zgłaszającym się do niego podmiotom, m.in. co do możliwości udostępniania danych pomiędzy urzędem gminy a ośrodkiem pomocy społecznej.

Należy podkreślić, że GIODO nie prowadzi żadnych postępowań skargowych związanych z Programem Rodzina 500+. Niemniej, na podstawie pozyskiwanych sygnałów, kataloguje zakres zagadnień, które mogą być przedmiotem ewentualnych prac legislacyjnych zmierzających do doskonalenia przepisów ustawy o pomocy państwa w wychowywaniu dzieci np. na etapie ich ewaluacji.

Jak zmienia się w Polsce podejście do ochrony danych osobowych? Czy jest lepiej czy wręcz przeciwnie?

– Biorąc pod uwagę badania Eurobarometru oraz rosnącą z roku na rok liczbę kierowanych do GIODO skarg, można by przypuszczać, że świadomość Polaków w zakresie ochrony danych osobowych i prywatności jest coraz wyższa. Jednak w mojej opinii, jest ona bardzo powierzchowna. Chciałabym, 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. Wiedza na ten temat wciąż jest zbyt mała.

GIODO od lat prowadzi szeroko zakrojoną działalność edukacyjną skierowaną do różnych grup odbiorców. Z myślą o najmłodszych realizowany jest ogólnopolski program edukacyjny dla szkół i nauczycieli „Twoje dane – Twoja sprawa”. Dla administratorów bezpieczeństwa informacji (ABI) utworzyliśmy serwis, w którym znajdują się informacje i porady dotyczące m.in. powołania i rejestracji ABI oraz wykonywania przez niego jego ustawowych obowiązków. Warto też wspomnieć o platformie edukacyjno-informacyjnej eduGIODO, czyli internetowym serwisie, adresowanym zarówno do administratorów danych, jak również do każdej osoby, której dane dotyczą.

Jakie zmiany prawne należałoby wprowadzić, w szczególności w sferze samorządu terytorialnego, by ochrona danych osobowych była jeszcze lepsza?

– Obecnie największym wyzwaniem będzie przygotowanie się do stosowania przepisów ogólnego rozporządzenia o ochronie danych osobowych. Mimo że będzie ono stosowane bezpośrednio, to do jego przepisów musimy dostosować całe polskie prawo. W tym celu konieczne będzie dokonanie przeglądu wielu aktów prawnych, m.in. po to, aby ujednolicić definicje i wprowadzić nowe. Ponadto rozporządzenie przewiduje także przypadki, kiedy poszczególne kwestie pozostawione są do uregulowania lub doprecyzowania przez prawo krajowe. Przykładowo są to m.in. takie szczegółowe zagadnienia sektorowe, jak chociażby przetwarzanie danych osobowych na potrzeby zatrudnienia czy ochrony zdrowia.

Z kolei podmioty przetwarzające dane muszą przygotować się m.in. do zmian w procedurach i zasadach przetwarzania danych. Dla podmiotów z sektora publicznego istotny może być zaś obowiązek zatrudnienia Data Protection Officera, czyli inspektora ochrony danych. Taką funkcję pełni obecnie administrator bezpieczeństwa informacji (ABI) – jednak jego powołanie jest dobrowolne. Po wejściu w życie unijnego rozporządzenia, wszystkie instytucje publiczne będą musiały mieć w swoich strukturach DPO.

Dziękuję za rozmowę.