

Status ABI po wejściu RODO

Rozmowa z Moniką Młotkiewicz, zastępcą dyrektora Departamentu Rejestracji ABI i Zbiorów Danych Osobowych w Biurze GİODO.

Rozmawia: Dominik Krzysztofowicz

Od 25 maja rolę administratorów bezpieczeństwa informacji (ABI) przejmą inspektorzy ochrony danych (IOD). Jakie są różnice pomiędzy nimi?

W Polsce jesteśmy w o tyle korzystnej sytuacji, że przepisy obecnej ustawy o ochronie danych osobowych dotyczące ABI uległy dużej zmianie na początku 2015 roku i są bardzo zbliżone do tych uregulowań, które zawiera unijne rozporządzenie o ochronie danych (RODO) w stosunku do inspektorów ochrony danych. Niemniej jednak przepisy RODO jeszcze bardziej wzmacniają pozycję inspektorów, dają im więcej gwarancji niezależności. Zmieniają też katalog zadań inspektora, rozszerzając go o pewne nowe obowiązki. Generalnie inspektorzy będą pełnić trzy role. Pierwsza to rola audytora i osoby monitorującej, czy przepisy dotyczące ochrony danych osobowych są przestrzegane przez administratora danych i jego pracowników. Druga ma charakter edukacyjno-informacyjny. Wypełniając ją, IOD będzie informować administratora danych, czyli kierownika jednostki i jego pracowników o nowych obowiązkach, tłumaczyć ich sens i doradzać, np. w ocenie skutków działań. Trzecia, bardzo ważna, to rola pośrednika między administratorem danych, organem nadzorczym i osobami, których dane dotyczą. Każda osoba, której dane są przetwarzane, może bowiem kontaktować się z IOD w każdej sprawie dotyczącej przetwarzania jej danych.

Do tej pory różne osoby pełniły funkcję administratorów bezpieczeństwa informacji. Wiele z nich sygnalizuje nam swoje wątpliwości co do dalszego pełnienia funkcji inspektorów ochrony danych po 25 maja.

Rzeczywiście, podczas konferencji lub na szkoleniach podchodzą do mnie osoby, którym funkcja ABI została narzucona, dołożona do dotychczasowych pełnoetatowych obowiązków. Skarżą się też, że do jej pełnienia nie miały przygotowania, a środki finansowe na ten cel nie były im zapewnione, mimo ustawowego obowiązku. Wskazują też na brak zrozumienia i wsparcia ze strony nie tylko kierownictwa, ale też innych osób zatrud-

nionych w instytucji. Takie podejście jest zupełnie niezrozumiałe w kontekście wzmocnienia znaczenia tej funkcji przez nowe unijne przepisy.

Często zdarza się, że pełnienie funkcji inspektora może powodować konflikt interesów. Czy na przykład sekretarz gminy może być inspektorem ochrony danych?

W wielu jednostkach samorządowych sekretarz gminy pełni funkcję ABI, bo jest osobą, która spełnia warunek bezpośredniej podle-



głości kierownictwu urzędu. Niemniej jednak i na gruncie obecnych przepisów, i na gruncie RODO, istnieje zakaz łączenia funkcji ABI z takimi innymi, które powodują nadmierne obciążenie lub właśnie konflikt interesów. Najkrócej mówiąc, chodzi o to, żeby osoba, która podejmuje decyzje w zakresie celów i sposobów przetwarzania danych, nie dokonywała następnie oceny tych decyzji pod kątem ich zgodności z przepisami prawa.

A informatycy? W wielu urzędach to oni pełnią funkcję ABI, a już niedługo będą pełnić rolę inspektorów ochrony danych. Nie ma tu konfliktu interesów?

W dużej mierze zależy to od odpowiedzi na pytanie o zakres obowiązków informatyka. Istnieje na przykład problem łączenia funkcji IOD z tak zwanym ASI, czyli administratorem systemów informatycznych. Choć, poza drobnymi wyjątkami, nie ma przepisów definiujących funkcję ASI, to najczęściej do osób ją sprawujących należy m.in. określanie sposobów zabezpieczeń w systemach informatycznych czy identyfikacja potencjalnych zagrożeń i podatności dla systemów informatycznych oraz sposobów ich eliminowania. Jeśli ktoś podejmuje decyzje w tym zakresie, to nie może ich potem weryfikować w kontekście przepisów ochrony danych osobowych – bo kontrolowałby sam siebie. Wszystko zależy więc od tego, czym w konkretnym przypadku zajmuje się informatyk. Nie można jednoznacznie wykluczyć możliwości wykonywania przez niego funkcji IOD, bo wykształcenie informatyczne jest w tym przypadku bardzo przydatne.

Wyobrażam sobie sytuację, kiedy kierownik małej jednostki przychodzi do informatyka zajmującego się głównie podłączaniem myszek i wysyłaniem maili i wyznacza mu odpowiedzialną rolę IOD, niekoniecznie wiedząc, „z czym to się je”...

Tak, to już się dzieje w przypadku powoływania ABI. W samorządach ta funkcja często jest przypisywana osobie na zasadzie arbitralnej dyspozycji pracodawcy. Tak nie powinno być, bo ta funkcja wymaga odpowiednich predyspozycji, przygotowania i zaangażowania. Ponadto szeregowy pracownik – a takim najczęściej jest informatyk – nie spełnia wymogu podległości bezpośrednio kierownictwu jednostki.

Do tej pory powoływanie ABI było w samorządach dobrowolne, od 25 maja będzie obowiązkiem powołania IOD. Jakie jeszcze różnice widać między RODO a dotychczasową ustawą o ochronie danych osobowych?

Rozporządzenie wzmacnia rolę inspektorów ochrony danych, którzy we wszystkich państwach członkowskich UE mają tworzyć skuteczny system ochrony danych osobowych. Osoby pełniące tę funkcję zyskują większe gwarancje niezależności, a obowiązkiem kierownictwa jest zapewnienie im odpowiedniego wsparcia. W Polsce, jak wspominałam, sytuacja jest o tyle korzystna, że wiele rozwiązań przewidzianych w RODO powinno być już w tej chwili stosowanych, bo zostały uwzględnione w przepisach ustawy o ochronie danych osobowych.

Dzięki temu będzie nam łatwiej wdrożyć RODO?

Na pewno znacznie łatwiej, ale – jak wspominałam – rozporządzenie dodatkowo wzmacnia pozycję inspektorów ochrony danych. Wprowadza kilka istotnych obowiązków dla administratorów danych, którzy będą musieli wspierać swoich IOD, np. dostarczając im środki na podnoszenie wiedzy. RODO to regulacja, która ma być aktualna przez dziesiątki lat, w związku z tym przewiduje obowiązek dostosowywania jednostki, w której pracuje IOD, do zmieniającej się rzeczywistości, np. technologicznej. Wiąże się z tym potrzeba ciągłego aktualizowania wiedzy. ABI przygotowujący się do roli IOD powinni z tego korzystać, domagać się, by w budżecie jednostki były zagwarantowane środki na edukację, szkolenia.

Kierownicy jednostek zgodnie z przepisami powinni, czy też mają obowiązek podnoszenia wiedzy IOD? Jak to jest sformułowane w RODO?

Przepis jasno formułuje tę kwestię, nie pozostawiając wątpliwości, że jest to obowiązek prawny administratora. Art. 38 ust. 2 stanowi, że administrator oraz podmiot przetwarzający wspierają inspektora ochrony danych w wypełnianiu przez niego zadań, o których mowa w art. 39, zapewniając zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej. Nie ma tu miejsca na wątpliwości. Szefowie różnych organizacji, w tym jednostek samorządowych, muszą mieć tego świadomość. Wskazujemy na to również w komunikacie opublikowanym w ostatnich dniach na stronie internetowej urzędu: www.giodo.gov.pl.

RODO przewiduje więcej rozwiązań podnoszących status obecnych ABI, a przyszłych IOD?

Oczywiście. Jednym z ważniejszych jest przepis, zgodnie z którym nie wolno wyda-

wać instrukcji inspektorowi, zarówno co do wykonywanych przez niego zadań, jak i treści opinii oraz tego, w jakich sprawach powinien je wydawać. To rozwiązanie zbliżone do tego, które funkcjonuje w przypadku zawodów zaufania publicznego, np. radcy prawnego, gdzie niezależność i przestrzeganie zasady praworządności w wykonywaniu zadań są bardzo ważne. Wszystkie opinie wydawane przez IOD mają być wydawane w sposób niezależny. Kolejne istotne rozwiązanie to zakaz odwoływania inspektora i karania go za wykonywanie funkcji. Nie trzeba tłumaczyć, że funkcja wewnętrznego audytora nie jest łatwa. Jego rolą jest wska-

Bardzo ważny jest zakaz odwoływania inspektora. Nie trzeba tłumaczyć, że funkcja wewnętrznego audytora nie jest łatwa. Jego rolą jest wskazywanie nieprawidłowości, domaganie się zmian, niekiedy pociągających za sobą konieczność poniesienia kosztów. Pokusa, by takiej osoby się pozbyć, może być duża, stąd konkretne rozwiązanie prawne, które ma ją chronić.

zywanie nieprawidłowości, domaganie się zmian niekiedy pociągających za sobą konieczność ponoszenia kosztów. Pokusa, by takiej osoby się pozbyć, może być duża, stąd konkretne rozwiązanie prawne, które ma ją chronić.

RODO przewiduje możliwość zatrudnienia kogoś z zewnątrz, osoby, która może obsługiwać kilka jednostek. Czy ten temat pojawia się w rozmowach z samorządowcami? Oczywiście, jest duże zainteresowanie takim rozwiązaniem, szczególnie w mniejszych samorządach, które mają niewielkie

zasoby kadrowe i możliwości finansowe i w związku z tym chcą zatrudniać wspólnie jednego IOD. W wielu przypadkach to się sprawdzi. Szczególnie jeśli podmioty współpracują i realizują te same zadania. Ważne jednak, żeby decyzja została podjęta świadomie i z rozważą. IOD musi mieć takie warunki funkcjonowania, które pozwolą mu na rzeczywiste i prawidłowe realizowanie obowiązków wynikających z przepisów. Musi też znać szczegóły funkcjonowania danej organizacji. Jeśli więc, pracując dla kilku podmiotów, rzeczywiście będzie w stanie służyć im fachową pomocą, to można się na to zdecydować.

Jak to zrobić?

Gdy już wybierzemy odpowiednią osobę, trzeba pamiętać, że jeśli ma ona pełnić funkcję IOD w kilku podmiotach, to każdy administrator, czyli szef jednostki, musi oddzielnie ją do tego wyznaczyć i zgłosić do organu nadzorczego. Trzeba też ustalić, jaka będzie podstawa świadczenia przez nią pracy oraz wymiar czasu poświęcanego na rzecz każdego z podmiotów. Konieczne może być wyznaczenie w każdym podmiocie osób stale współpracujących z inspektorem. Należy to tak zorganizować, aby bieżące monitorowanie zgodności przetwarzania danych z prawem oraz inne obowiązki inspektora wskazane w RODO mogły być faktycznie realizowane wobec każdego z administratorów, który korzysta z pracy jednej, tej samej osoby.

Takie rozwiązanie sprawdzi się w każdym przypadku?

Zdecydowanie nie. To dobre dla niewielkich jednostek. Im większe podmioty i większe wyzwania w zakresie ochrony danych, tym większe ryzyko, że się nie sprawdzi.

Co to znaczy duża jednostka?

To kwestia ocenna. Decydujące znaczenie ma to, by była właściwie obsłużona.

Zapytam inaczej: jeśli zgłosi się do państwa sześć sąsiadujących ze sobą gmin, które chcą skorzystać z takiego modelu, to co państwo im poradzą?

Dostajemy takie pytania, ale uciekamy od konkretnych odpowiedzi, bo nie możemy ich dać, jeśli przepis nie stanowi wyrażnie, że maksymalnie to może być tyle i tyle podmiotów. Należy zastosować kryterium jakościowe. Jeśli chcemy mieć dobrego inspektora i właściwy, fachowy nadzór nad sferą obowiązków wynikających z RODO, to zrobimy to rzetelnie i odpowiedzialnie. Będzie to oczywiście kosztować więcej, ale zyskamy pewność, że działa. ■