

Inspektorzy GIODO sprawdzają, jak kancelarie chronią dane klientów

KONTROLE! O zaplanowanych na 2016 rok tzw. kontrolach sektorowych oraz tych przeprowadzonych przy udziale administratorów bezpieczeństwa informacji (ABI) mówi dr Edyta Bielak-Jomaa, generalny inspektor ochrony danych osobowych.



EDYTA BIELAK-JOMAA

W: Generalny inspektor ochrony danych osobowych planuje w tym roku skoncentrować się na kontroli kilku sektorów. Czy może pani zdradzić jakich?

EDYTA BIELAK-JOMAA: Podejmując decyzję, które sektory i instytucje zostaną objęte kontrolą GIODO w 2016 r., braliśmy pod uwagę kilka aspektów. Jeden to prowadzenie działalności związanej z przetwarzaniem bardzo specyficznych danych osobowych, np. należących do kategorii danych wrażliwych. Kolejny to wzrost zagrożeń dotyczących ochrony danych osobowych, spowodowany m.in. postępem technologicznym czy zmianą przepisów, co wymuszało na administratorach danych wprowadzanie nowych sposobów i zasad przetwarzania danych. Z kolei wyznaczenie niektórych kategorii organów publicznych, których będą dotyczyły kontrole sektorowe, podyktowane było nowymi zadaniami nałożonymi na generalnego inspektora ochrony danych osobowych przepisami prawa europejskiego.

Będziemy więc sprawdzać poszczególne instytucje i firmy pod kątem zgodności przetwarzania przez nie danych osobowych z przepisami prawa. Wśród kontrolowanych podmiotów znajdują się więc m.in. organy uprawnione do korzystania z Systemu Informacji Celnej. Chodzi o organy celne i organizacje, które uzyskały zezwolenie na korzystanie z tego systemu. Następnie będą to organy przetwarzające dane osobowe w Systemie Informacyjnym Schengen

➔ Zgodnie z przepisami

Zgodnie z art. 19b ustawy o ochronie danych osobowych GIODO może się zwrócić do administratora bezpieczeństwa informacji wpisanego do rejestru, o którym mowa w art. 46c, o dokonanie sprawdzenia, o którym mowa w art. 36a ust. 2 pkt 1 lit. a, u administratora danych, który go powołał, wskazując zakres i termin sprawdzenia. Po dokonaniu takiego sprawdzenia administrator bezpieczeństwa informacji, za pośrednictwem administratora danych, przedstawia GIODO sprawozdanie. Dokonanie przez administratora bezpieczeństwa informacji sprawdzenia nie wyłącza prawa GIODO do przeprowadzenia kontroli, o której mowa w art. 12 ustawy. ■

i Wizowym Systemie Informacyjnym, a także podmioty przetwarzające dane w systemie Eurodac.

Kontrolą sektorową chcemy także objąć starostwa powiatowe, przy czym najbardziej będzie nas interesowało to, w jaki sposób przebiega proces przetwarzania danych w wydziałach geodezji. Powodem skoncentrowania się akurat na tego rodzaju aktywności starostw są docierające do GIODO sygnały związane z nieprawidłowościami w tym obszarze.

Jeśli zaś chodzi o przedsiębiorców, to z ich punktu widzenia istotna może być informacja, że grupa wytypowana do czynności kontrolnych są kancelarie prawne. W ich przypadku chcemy skoncentrować się na tym, w jaki sposób zabezpieczają one dane osobowe swoich klientów oraz w jaki sposób przebiega proces przetwarzania informacji na mocy umowy powierzenia lub outsourcingu. Okazuje się, że inspekcje w tym sektorze spełniają też społeczne oczekiwania.

W jaki sposób będą wybierane konkretne podmioty, które mają być kontrolowane?

Część podmiotów wybierzemy losowo, a część zostanie poddana kontroli w wyniku wpływających do nas skarg. Jeszcze inne mogą zostać wytypowane na skutek doniesień medialnych. Co istotne, kontrolerzy mogą też zapukać do tych administratorów danych, u których wprowadzie już kiedyś kontrole się odbyły, ale znacząco zmieniły się okoliczności przetwarzania danych, o których mówiłam.

Jedną z ostatnich nowelizacji ustawy o ochronie danych osobowych znacząco wpłynęła na zmianę roli i pozycji tzw. administratorów bezpieczeństwa informacji. Czy to ich nowe ustrukturyzowanie w strukturze organizacyjnej i wiedza, którą

zgodnie z przepisami powinni dysponować, zostanie przez urząd wykorzystana?

Zgodnie ze zmianami, wprowadzonymi w 2015 roku do ustawy o ochronie danych osobowych, to na ABI spoczywa obowiązek zagwarantowania zgodnego z prawem procesu przetwarzania danych osobowych w instytucji, w której został powołany. Na jego wiedzy i doświadczeniu powinien opierać się więc administrator danych, zapewniając mu jednocześnie niezbędne warunki potrzebne dla odpowiedniego wykonywania jego obowiązków. GIODO, wykorzystując tę nową rolę i zadania ABI, będzie właśnie za jego pośrednictwem współpracował z administratorem danych. Chcemy na większą skalę uruchomić procedurę tzw. wystąpienia o dokonanie sprawdzeń na zlecenie GIODO.

Czy tutaj też zostały wytypowane jakieś szczególne branże, na których GIODO będzie się koncentrować?

Wystąpienia o dokonanie sprawdzeń, jeżeli tylko zaistnieją do tego przesłanki, będą doraźnie kierowane do różnych podmiotów, na wniosek dyrektorów departamentów Biura Generalnego Inspektora Ochrony Danych lub organów władzy publicznej. Jednak naszą szczególną uwagę chcemy w tym roku skoncentrować na bankach, towarzystwach ubezpieczeniowych oraz gminach.

W przypadku pierwszej grupy najbardziej będzie nas interesowała polityka w zakresie rozpatrywania sprzeciwów klientów wobec przetwarzania danych osobowych w celach marketingowych.

W przypadku drugiej grupy planujemy zwrócenie się do administratorów bezpieczeństwa informacji z wnioskiem o przeprowadzenie sprawdzenia, w jaki sposób przetwarzane są dane o stanie zdrowia w związku z oferowanymi przez te podmioty ubezpieczeniami zdrowotnymi.

Natomiast w przypadku gmin będziemy się chcieli skoncentrować na realizowanym przez te podmioty obowiązkowi informacyjnym, który nie zawsze bywa wypełniany.

Czy taki wniosek (wystąpienie) o dokonanie sprawdzenia może potencjalnie wpłynąć do każdego administratora danych?

Nie, bowiem GIODO może wystąpić o przeprowadzenie sprawdzenia wyłącznie do ABI, a nie do administratora danych. Warto przypomnieć, że ABI, do którego GIODO kieruje swój wniosek, musi być przez administratora danych osobowych powołany, a ponadto zgłoszony i wpisany do prowadzonego przez GIODO specjalnego rejestru. Wskazuje na to wprost art. 19b ust. 1 ustawy o ochronie danych osobowych.

Czy ABI, do którego wpłynie taki wniosek, będzie musiał całościowo ocenić procedury przetwarzania danych u konkretnego administratora?

GIODO może zwrócić się do ABI o sprawdzenie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych u danego administratora danych, przy czym powinien sprecyzować, w jakim zakresie działania te powinny zostać podjęte i w jakim terminie zakończone.

Jak podkreśla się w doktrynie, zakres sprawdzenia powinien zostać wskazany przez odniesienie do konkretnych kwestii budzących wątpliwości organu np. w związku z wniosoną do niego skargą na danego administratora danych. Może on zatem zostać wyznaczony przez wskazanie konkretnego zagadnienia (np. monitoringu wizyjnego), kategorii danych osobowych (np. danych biometrycznych, danych tzw. wrażliwych), realizacji określonego obowiązku wynikającego z przepisu prawa (np. realizacji obowiązku informacyjnego), konkretnego zbioru danych osobowych (np. zbioru kadrowo-płacowego, zbioru klientów) lub systemu informatycznego.

Czy istnieje jeden z góry określony termin, w jakim ABI powinien przygotować i przekazać przygotowane przez siebie sprawozdanie?

Termin ten jest określany odrębnie w każdym wystąpieniu, z uwzględnieniem czasu, jaki

➔ Zakres sprawozdania

Zgodnie z art. 36c ustawy o ochronie danych osobowych (DzU z 2014 r., poz. 1182 ze zm.) sprawozdanie stanowi dokument opracowany przez ABI po dokonaniu sprawdzenia i powinno zawierać:

- oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania,
 - imię i nazwisko administratora bezpieczeństwa informacji,
 - wykaz czynności podjętych przez administratora bezpieczeństwa informacji w toku sprawdzenia oraz imiona, nazwiska i stanowiska osób biorących udział w tych czynnościach,
 - datę rozpoczęcia i zakończenia sprawdzenia,
 - określenie przedmiotu i zakresu sprawdzenia,
 - opis stanu faktycznego stwierdzonego w toku sprawdzenia oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
 - stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych w zakresie objętym sprawdzeniem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem,
 - wyszczególnienie załączników stanowiących składową część sprawozdania,
 - podpis administratora bezpieczeństwa informacji, a w przypadku sprawozdania w postaci papierowej – dodatkowo parafy administratora bezpieczeństwa informacji na każdej stronie sprawozdania,
 - datę i miejsce podpisania sprawozdania przez administratora bezpieczeństwa informacji.
- ABI przysyła sprawozdanie generalnemu inspektorowi ochrony danych osobowych za pośrednictwem administratora danych. Powinno ona zostać sporządzona w postaci elektronicznej albo w postaci papierowej z zachowaniem terminu wskazanego przez GIODO. W praktyce może to wyglądać w ten sposób, że sprawozdanie ze sprawdzenia podpisuje ABI, ale pismo przewodnie, do którego to sprawozdanie jest załączone, podpisuje administrator danych lub osoba przez niego upoważniona. ■

w konkretnym przypadku jest niezbędny do dokonania sprawdzenia i przygotowania sprawozdania. Chodzi nam o to, aby były to dokumenty kompletne i dobrze przygotowane, a niekoniecznie wykonane w jak najkrótszym czasie.

Czy sprawozdanie kończy postępowanie?

Dokonanie przez ABI sprawdzenia nie wyłącza możliwości przeprowadzenia przez inspektorów GIODO kontroli na zasadach ogólnych, określonych w art. 12 i następnych ustawy. Może się zdarzyć, że dokonanie sprawdzenia przez ABI i przedstawienie sprawozdania wręcz stanie się impulsem do przeprowadzenia takiej kontroli. Zakładam jednak, że takie działanie będzie rzadkością, generalnie zaś stosowany będzie któryś z dwóch możliwych scenariuszy.

Jeżeli sprawozdanie ze sprawdzenia będzie zawierało wszystkie elementy wymienione w art. 36c ustawy o ochronie danych osobowych oraz brak będzie podstaw do stwierdzenia naruszenia przepisów, GIODO w zakresie wskazanym w wystąpieniu poinformuje administratora danych o braku zastrzeżeń odnośnie do sprawozdania.

Jeżeli natomiast sprawozdanie nie będzie spełniać wszystkich wymogów określonych w powołanym artykule lub wszystkich niezbędnych dowodów będących podstawą ustaleń zamieszczonych w sprawozdaniu, GIODO wezwie ABI do ich uzupełnienia wraz z podaniem terminu.

Czy ABI są przygotowani do prowadzenia takich sprawdzeń, czy wiedzą, jak powinni postępować, jakie mają uprawnienia?

Zakładam, że ABI znają swoje wyznaczone przepisami prawa, obowiązki i uprawnienia. Posiadanie odpowiedniej wiedzy w zakresie ochrony danych osobowych to przecież warunek, który muszą spełnić, aby administrator danych mógł ich na to stanowisko powołać. Ponieważ jednak nowe rozwiązania prawne budzą pewne wątpliwości interpretacyjne, na naszej stronie internetowej uruchomiliśmy „ABI-informator” – specjalny serwis opisujący m.in. status i zadania ABI. Jedną z jego części są też odpowiedzi na najczęściej zadawane pytania. Dostępny jest pod adresem <https://abi.giodo.gov.pl> ©

—rozmawiał Michał Koltuniak