

# Administrator bezpieczeństwa informacji powinien być jak inspektor

**DANE OSOBOWE** 1 stycznia 2015 r. wejdą w życie zmienione przepisy ustawy o ochronie danych osobowych. Modyfikują one rolę i pozycję administratora bezpieczeństwa informacji (ABI) oraz zasady rejestrowania zbiorów.

**W:** Czy po nowelizacji przepisów ustawy o ochronie danych osobowych każdy administrator danych musi powołać u siebie administratora bezpieczeństwa informacji?

**ANDRZEJ LEWINSKI:** Absolutnie nie. Decyzja należy do administratora danych, czyli każdej osoby lub instytucji, która decyduje o celach i środkach przetwarzania takich informacji. Jeżeli administrator uzna, że jest w stanie samodzielnie zadbać o prawidłowe przetwarzanie danych i zapanować nad tym procesem, to nie ma takiego obowiązku. Jednak może to zrobić, a w pewnych przypadkach powinien.

## Powinien?

Tak. Warto bowiem zauważyć, że w społeczeństwie rośnie świadomość potrzeby ochrony danych i zasad z tym związanych. Świadczy o tym chociażby liczba skarg, jakie wpływają do generalnego inspektora ochrony danych osobowych (GIODO), w których skarżący zawiadamiają o nieprawidłowym przetwarzaniu ich danych. Wiele z tych skarg jest uzasadnionych, jednocześnie świadomość po stronie samych administratorów danych nadal pozostawia wiele do życzenia. W wielu przypadkach, chociaż ustawa o ochronie danych osobowych obowiązuje już od 17 lat, nie znają oni podstawowych obowiązków, jakie nakładają na nich jej przepisy. Dlatego warto, aby korzystali z pomocy osób mających wiedzę na ten temat, czyli ABI. Należy bowiem podkreślić, że chodzi tutaj o osoby, które odpowiadają nie tylko za kwestie techniczne, związane np. z prawidłowym zabezpieczeniem systemów informatycznych, szyfrowaniem danych, dbaniem o to, aby nie były one narażone na ataki cyberprzestępców. ABI ma bowiem odpowiadać za całokształt prawidłowego przetwarzania danych, a więc zarówno za ich ochronę, jak i szkolenia oraz doradzanie innym pracownikom administratora, mającym do nich dostęp. ABI ma nadzorować cały proces przetwarzania danych. Powinien być więc takim „wewnętrznym inspektorem ochrony danych”.

**To może się kojarzyć ze zwiększaniem obowiązków nakładanych na przedsiębiorców i wzrostem kosztów ich działalności.**

Nie bardziej mylnego. Przecież żadne dodatkowe obowiązki na przedsiębiorców, którzy w swojej działalności wykorzystują dane, nie zostają tą nowelizacją narzucone. Do tej pory wielu z nich po prostu naruszało przepisy ustawy, nie stosując wielu jej zasad, a teraz mają szansę i muszą to naprawić. Proszę zwrócić uwagę, że w Polsce mamy co najmniej 2 miliony administratorów danych, a do GIODO zgłoszono 200 tys. zbiorów danych, czyli zrobiło to 10 proc. administratorów. Czy to znaczy, że pozostałe 90 proc. ma prawo nie zgłaszać zbiorów danych na podstawie art. 43 ustawy czy po prostu nie wiedzą o tym, że powinni to zrobić? Nie zdają sobie sprawy, iż niezarejestrowanie zbioru danych to odpowiedzialność karna z art. 53 ustawy o ochronie danych osobowych. A to przecież niejedyny rodzaj naruszenia, z jakim się spotykamy.

**Może nie chcą się po prostu ujawniać? I nadal będą tak robić?**

Takie działanie jest nielegalne i grozi odpowiedzialnością karną. Ponadto wszyscy administratorzy powinni mieć świadomość, że już wkrótce wejdą w życie zupełnie nowe przepisy o ochronie danych osobowych.



Chodzi tutaj o unijne rozporządzenie w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych, którego projekt jest już w zasadzie gotowy, a prace nad dopracowaniem jego ostatecznej wersji idą bardzo sprawnie. Rozporządzenie zmieni i ujednolici reguły ochrony danych osobowych w całej Unii Europejskiej. I, co bardzo istotne, przewiduje ono surowe kary finansowe za naruszenie przepisów. W pewnych przypadkach mowa jest nawet o 100 mln euro! Jeżeli wejdą one w życie, to automatycznie będą stosowane także w Polsce.

## To brzmi niemal jak groźba.

Nie chodzi o to, aby kogokolwiek straszyć. Kto nie narusza przepisów, na żadne sankcje się nie naraża. Kto zechce ich uniknąć, a nie jest pewien swojej wiedzy z zakresu ochrony danych, może powołać u siebie administratora bezpieczeństwa informacji, który powinien posiadać wiedzę w tym zakresie, do czego zobowiązują nowe przepisy. Warto skorzystać z tej instytucji i potraktować okres między nowelizacją naszych krajowych przepisów a wejściem w życie unijnego rozporządzenia, jako czas na naukę i zbieranie doświadczeń. Wówczas wizja kar finansowych nie będzie straszna. Poza tym ABI nie jest zupełnie nieznanym i nowym tworem, bowiem unijna dyrektywa (95/46/WE), która w tej chwili harmonizuje prawo europejskie, i na podstawie której wydana została polska ustawa o ochronie danych osobowych, przewiduje możliwość powołania urzędnika odpowiedzialnego za ochronę danych. Taka konstrukcja została wprowadzona w większości państw członkowskich UE. ABI w dotychczasowych przepisach art. 36 ust. 3 mógł być wyznaczony. Nowe przepisy dały mu uprawnienia i wzmocniły jego status.

**I zapewne taka konstrukcja zostanie powtórzona w rozporządzeniu, o którym pan wspominał?**

Tak. Już w preambule, w motywie 75, mowa jest o tym, że jeśli przetwarzanie danych odbywa się w sektorze publicznym lub jeśli przetwarzanie w sektorze gospodarczym prowadzi duże przedsiębiorstwo albo główna działalność firmy, niezależnie od jej wielkości, obejmuje operacje przetwarzania, które wymagają regularnego i systematycznego monitorowania, osoba trzecia powinna wspomagać administratora lub podmiot przetwarzający w monitorowaniu zgodności na poziomie wewnętrznym z przepisami rozporządzenia. Taki inspektor ochrony danych, jak dalej wskazuje ten projekt, może być pracownikiem administratora oraz powinien być w stanie niezależnie wykonywać swoje obowiązki i zadania. Jak z tego wynika, wcześniej czy później, konieczność powołania ABI i tak może się pojawić.

**Ustawa wskazuje na pewne wymogi, które muszą być spełnione przy powoływaniu takiego administratora.**

**•O nowych zadaniach ABI oraz o przyszłości przepisów o ochronie danych osobowych mówi Andrzej Lewiński, zastępca Generalnego Inspektora Ochrony Danych Osobowych.**

Tak. Z jednej strony chodzi m.in. o to, aby taka osoba legitymowała się wyższym wykształceniem, korzystała z pełni praw publicznych, nie była karana za przestępstwo popełnione z winy umyślnej oraz miała odpowiednią wiedzę z zakresu przepisów o ochronie danych osobowych. Z drugiej, aby była odpowiednio umiejscowiona w strukturze podmiotu, w którym działa. Musi podlegać bezpośrednio kierownikowi danej jednostki. Nie można tworzyć szczebli pośrednich. Wszystko po to, aby pozycja tej osoby była naprawdę mocna. Dyrektywa wymaga niezależności takiej osoby. Należy jednak podkreślić, że ABI nie musi być pracownikiem danego administratora. Dopuszczalny jest tutaj tzw. outsourcing. Z kolei pracownik, gdyby został wyznaczony na takie stanowisko, mógłby wykonywać u danego pracodawcy także inne zadania, o ile nie kolidowałyby to z jego obowiązkami w zakresie ochrony danych osobowych.

**Co należy rozumieć pod pojęciem odpowiednich kwalifikacji do zajmowania stanowiska ABI?**

Ustawa tego nie precyzuje. I zresztą o to chodziło. Celem nowelizacji nie było tworzenie nowej grupy zawodowej, co stałoby w sprzeczności z ogólnym trendem do deregulacji zawodów. To decyzja administratora, kogo powoła na takie stanowisko. Działając we własnym interesie, powinien powołać osobę, która ma rzeczywistą wiedzę z zakresu ochrony danych.

**Jak wynika z nowelizacji, GIODO może zlecić takiej osobie przeprowadzenie kontroli. Przecież w ten sposób ABI będzie tak naprawdę kontrolował samego siebie. Czy to w ogóle ma sens?**

## •NOWE PRZEPISY

Zgodnie z art. 36 ust. 1 ustawy o ochronie danych osobowych (DzU z 2014 r., poz. 1182) administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

W myśl ust. 2 administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, o których mowa powyżej. Następnie, zgodnie z ust. 3, administrator danych wyznacza administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad ochrony, o których mowa powyżej, chyba że sam wykonuje te czynności. Nowelizacja ustawy uchyla zacytowany ust. 3 i dodaje m.in. art. 36a, zgodnie z nim administrator danych może powołać administratora bezpieczeństwa informacji. Jego zadaniem jest zapewnienie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:

- sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych,
- nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2, oraz przestrzegania zasad w niej określonych,
- zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

Ponadto ABI będzie odpowiedzialny za prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1, zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt. 2–4a i 7. Zamiany w ustawie o ochronie danych osobowych są wynikiem ustawy z 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej. Wejdą w życie 1 stycznia 2015 r. ■

Proszę sobie wyobrazić, kiedy taka kontrola czy – mówiąc słowami ustawy – „sprawdzenie” może zostać zlecona. Najczęściej będzie to dotyczyło przypadków, w których do GIODO wpłynie skarga na działanie danego administratora. W takiej sytuacji nie chodzi przecież o to, żeby do przedsiębiorcy przysłali nasi inspektorzy i postraszyli karą. Chodzi przede wszystkim o to, aby proces przetwarzania danych był prawidłowy, aby chroniona była prywatność i bezpieczeństwo wszystkich osób, których danymi dysponuje administrator. Dlatego ABI ma sprawdzić, czy doszło do naruszenia procedur, a jeżeli skarga była uzasadniona, natychmiast wprowadzić rozwiązania naprawcze. Kontroluje on w imieniu administratora danych wszystkich. Jednak pragnę zauważyć, że w przypadku, gdy w naszej opinii skarga była uzasadniona, a ABI powie nam, że wszystko jest w porządku, to GIODO ma prawo przeprowadzić własną kontrolę. Jej odmienny wynik może być jasnym sygnałem dla administratora, że wyznaczony przez niego ABI nie do końca spełnia wymogi ustawy, co do kwalifikacji. I tutaj wracamy do poprzedniego pytania. To praktyka będzie weryfikować kwalifikacje ABI.

**Co oprócz poczucia większego bezpieczeństwa, że proces operowania na danych jest prawidłowy, da przedsiębiorcy powołanie ABI?**

Przed wszystkim w takim przypadku odchodzimy od obowiązku rejestracji i aktualizacji zbiorów danych osobowych, o ile zbiór taki nie zawiera tzw. danych wrażliwych. Do tej pory, każdy administrator, który nie mógł skorzystać z wyłączenia na mocy art. 43, miał taki obowiązek. Jeżeli teraz zgłosi do GIODO powołanie administratora bezpieczeństwa informacji, który będzie spełniał ustawowe wymogi, z takiego obowiązku zostanie zwolniony. Innymi słowy, zamiast zgłaszać zbiór danych, administrator będzie zgłaszał ABI. Należy jednak jeszcze raz podkreślić, że nie dotyczy to administratorów danych wrażliwych, tj. np. takich, które ujawniają poglądy polityczne, dotyczą stanu zdrowia lub nalogów. W przypadku takich zbiorów ich rejestracja nadal będzie obowiązkowa, niezależnie od tego, czy administrator powoła ABI, czy nie.

—rozmawiał Michał Kołtuniak