

Administrator bezpieczeństwa informacji musi być niezależny

- ABI działa w ramach organizacyjnej odrębności.
- Firma ma obowiązek wyposażenia go w odpowiednie środki.
- Bezpośrednio podlega on kierownikowi jednostki lub administratorowi.

MICHAŁ KOŁTUNIAK

Powołanie administratora bezpieczeństwa informacji jest jedną z możliwości, jaką daje administratorowi danych w przedsiębiorstwie ustawa o ochronie danych osobowych (DzU z 2015 r., poz. 2135 ze zm.). Istnienie takiej osoby, która powinna mieć szeroką wiedzę z zakresu procedur związanych z ochroną danych i ich prawidłowego przetwarzania, daje administratorowi pewne przywileje. Jednym z nich jest zwolnienie z obowiązku rejestracji zbioru danych (tylko takiego, który nie zawiera informacji wrażliwych), jeżeli w myśl art. 40 ustawy taki obowiązek spoczywałby na przedsiębiorcy.

Inne przywileje wiążą się z przeniesieniem części bieżących obowiązków, które w normalnych warunkach spoczywają na administratorze danych, właśnie na ABI. Chociaż należy podkreślić, że niezależnie od tego, czy taka osoba funkcjonuje w firmie, czy też nie, i tak na administratorze danych spoczywa obowiązek przestrzegania reguł wynikających z ustawy. Mówiąc o bieżących obowiązkach, zgodnie z przepisami ABI powinien dbać o przestrzeganie przepisów o ochronie danych oraz prowadzić w określonych przypadkach ich rejestr (art. 36a ust. 2).

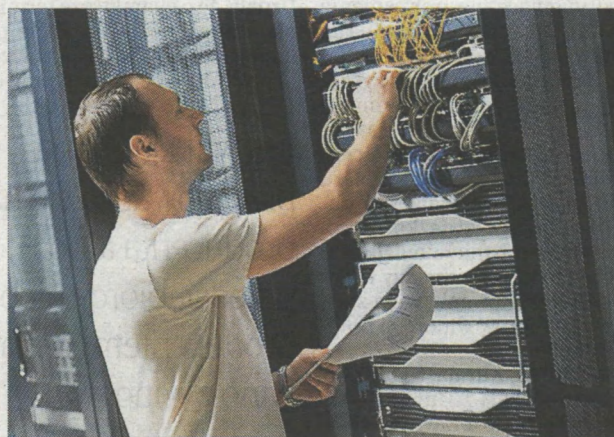
Zapewnienie przestrzegania przepisów oznacza:

- sprawdzanie zgodności przetwarzania danych z przepisami o ich ochronie oraz opracowanie w tym zakresie sprawozdania dla administratora danych,
- nadzorowanie opracowania i aktualizowania dokumentacji regulującej zasady przetwarzania danych w firmie (organizacji) i przestrzegania zasad w niej określonych,
- obowiązek zapoznawania osób upoważnionych do przetwarzania danych z przepisami w tym zakresie.

Jeżeli w firmie nie ma ABI, to wszystkie takie czynności, oprócz obowiązku przygotowania sprawozdania, wykonuje samodzielnie administrator.

Jeżeli przedsiębiorca decyduje się na powołanie ABI, to powinien mieć pełną zdolność do czynności prawnych, korzystać z pełni praw publicznych, posiadać wiedzę w zakresie ochrony danych, nie być karany za umyślne przestępstwo.

Ocena opisanych kompetencji i wiedzy kandydata na ABI należy wyłącznie do administratora danych, nie ma żadnych regulacji w tym zakresie. We własnym interesie administrator powinien zadbać o to, aby była to osoba z odpowiednim doświadczeniem.



♦ ABI powinien dbać o przestrzeganie przepisów o ochronie danych oraz prowadzić w określonych przypadkach ich rejestr

ABI w zakresie zapewniania przestrzegania przepisów o ochronie danych osobowych musi podlegać bezpośrednio kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej administratorem danych. Ten ostatni zobowiązany jest zaś do wyposażenia ABI w odpowiednie środki i zapewnienia mu organizacyjnej odrębności, co jest niezbędne do niezależnego wykonywania przez niego zadań.

Przez bezpośrednią podległość ABI kierownikowi jednostki organizacyjnej należy rozumieć, że w zakresie zapewniania przestrzegania przepisów o ochronie danych nie może on podlegać innym osobom niż kierownik jednostki organizacyjnej.

Jak wskazuje Andrzej Lewiński, zastępca generalnego inspektora ochrony danych osobowych – w interesie administratora jest, by ABI był faktycznie niezależny, czemu sprzyjać ma ustawowo gwarantowana bezpośrednia jego podległość kierownikowi zakładu. Tym samym ABI nie może

podlegać np. szefowi działu kadr, działu prawnego czy dyrektorowi ds. informatycznych. Tymczasem się zdarza, że na ABI powoływani są pracownicy pionów bezpieczeństwa, a czasem nawet ich wicedyrektorzy. To złe rozwiązanie, gdyż prowadzi do konfliktu interesów. Przecież zadaniem ABI jest m.in. kontrolowanie zabezpieczeń, a więc tak naprawdę zastępca sprawdza własnego szefa. Trudno wówczas o zapewnienie niezależności. Poprawnym rozwiązaniem jest taka organizacja pracy ABI, by w sprawach ochrony danych, był niezależny i podległy kierownictwu firmy – wyjaśnia Lewiński.

Z kolei wymóg zapewnienia ABI odrębności organizacyjnej umożliwia mu wykonywanie obowiązków niezależnie od pozostałych komórek organizacyjnych. Oznacza to, że ma on zapewnione środki organizacyjne i finansowe.

ABI może wykonywać także inne obowiązki w firmie, nie mogą one jednak kolidować z troską o ochronę i przetwarzanie danych. ©