Rola IOD przy naruszeniach ochrony danych osobowych

Posted on 2024-10-31

Rola inspektora ochrony danych (IOD) w zapewnieniu zgodności działań organizacji z przepisami RODO jest kluczowa. Jakie są jego obowiązki w przypadku naruszeń ochrony danych osobowych? Czy może działać w imieniu administratora? Wyjaśniamy, jakie zadania może w takich sytuacjach wykonywać, a jakich powinien unikać, aby nie naruszać przepisów prawa.

Jak IOD może wspierać administratora?

IOD jest ważnym uczestnikiem procesu zarządzania naruszeniami ochrony danych osobowych. Jego zadania w tym obszarze obejmują przede wszystkim:

- doradzanie administratorowi (art. 39 ust. 1 lit. a) RODO);
- monitorowanie zgodności działań podejmowanych przez administratora z przepisami RODO i przyjętymi procedurami (art. 39 ust. 1 lit. b) RODO);
- pełnienie funkcji punktu kontaktowego, od którego organ nadzorczy i osoby, których dane

dotyczą, mogą uzyskać dodatkowe informacje (art. 39 ust. 1 lit. e) RODO i art. 34 ust. 2 RODO w zw. z art. 33 ust. 3 lit. b) RODO);
- zwiększanie świadomości personelu administratora, organizowanie szkoleń oraz inne inicjatywy, które przyczyniają się do zapobiegania powstawaniu naruszeń ochrony danych osobowych (art. 39 ust. 1 lit. b) RODO).

Czego IOD powinien unikać?

Jednocześnie IOD nie może realizować obowiązków, za których wykonanie zgodnie z RODO odpowiada wyłącznie administrator. W praktyce oznacza to, że IOD nie powinien:

- zgłaszać naruszeń ochrony danych osobowych Prezesowi UODO w imieniu administratora, w tym także podpisywać i wysyłać takich zgłoszeń (art. 33 ust. 1 RODO);
- dokumentować naruszeń ochrony danych osobowych (art. 33 ust. 5 RODO);
- zawiadamiać osób, których dane dotyczą, o naruszeniach ochrony danych osobowych (art. 34 ust. 1 RODO);
- podpisywać pism, w których zobowiązuje się do podjęcia określonych działań w imieniu administratora, np. dotyczących bezpieczeństwa przetwarzania (art. 32 ust. 1 RODO);
- oraz w inny sposób działać na podstawie pełnomocnictwa udzielonego przez administratora w sprawach dotyczących ochrony danych osobowych.

Dlaczego nakładanie tych obowiązków na IOD jest

niewłaściwe?

Wykonywanie przez IOD zadań zarezerwowanych dla administratora jest sprzeczne z RODO i wywołuje pewne problemy:

• Ograniczenie niezależności: Udzielanie IOD pełnomocnictwa do działania w imieniu administratora narusza jego niezależność. Pełnomocnictwo wiąże się z koniecznością realizacji określonych poleceń, co stoi w sprzeczności z przepisami RODO, które zabraniają wydawania IOD instrukcji dotyczących wykonywania jego zadań (art. 38 ust. 3 RODO).

• Konflikt interesów: IOD ma nadzorować zgodność przetwarzania z przepisami o ochronie danych osobowych. Jeżeli samodzielnie realizuje zadania spoczywające na administratorze lub działa w jego imieniu, traci zdolność dokonywania obiektywnej oceny. Prowadzi to do konfliktu interesów. RODO zakazuje takich praktyk (art. 38 ust. 6 RODO).

Konsekwencje naruszania przepisów RODO

Łamanie przepisów dotyczących statusu IOD może mieć poważne konsekwencje dla organizacji. To m.in. utrata zaufania ze strony pracowników, klientów i partnerów biznesowych, ale także możliwość zastosowania przez Prezesa UODO uprawnień naprawczych, takich jak administracyjna kara pieniężna.

O czym warto pamiętać?

Podsumowując, IOD pełni w organizacji funkcję informacyjną, doradczą, monitorującą i nadzorczą. Aby skutecznie wykonywać swoje zadania, musi zachować autonomię, obiektywizm oraz unikać konfliktu interesów. Właściwe zrozumienie i respektowanie roli IOD to nie tylko wymóg prawny, ale także kluczowy element systemu bezpieczeństwa danych. Odpowiedni podział obowiązków pozwoli na efektywniejsze zarządzanie naruszeniami ochrony danych osobowych.