Rola kierownictwa administratora w procesie wykonywania przepisów RODO

Posted on 2024-05-31

RODO, które obowiązuje już sześć lat, nakłada na administratorów szereg rozmaitych obowiązków mających na celu ochronę osób fizycznych w związku z przetwarzaniem ich danych osobowych. Niestety, bezpieczeństwo danych wciąż nie jest traktowane priorytetowo przez organy kierownicze wielu organizacji.

Administrator jako organizacja

„Administrator” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych (art. 4 pkt 7 RODO). Cele i sposoby przetwarzania mogą też zostać określone bezpośrednio w prawie europejskim lub krajowym – wówczas administratora lub kryteria jego wyznaczania również można ustanowić poprzez normy prawne.

RODO zasadniczo nie stwarza ograniczeń dotyczących rodzaju podmiotu, który może pełnić funkcję administratora. Zazwyczaj jednak, choć nie zawsze, za administratora uznajemy organizację jako taką, a nie związaną z nią osobę fizyczną (np. pracownika, dyrektora lub prezesa zarządu spółki).

Rola kierownictwa administratora w procesie wykonywania przepisów RODO

Znaczenie kierownictwa administratora

Istotą roli administratora jest rzeczywista decyzyjność dotycząca kluczowych aspektów przetwarzania, dlatego szczególne znaczenie w tym procesie odgrywają organy kierownicze. Mimo to wciąż zdarza się, że ścisłe kierownictwo administratora przejawia daleko idącą nieświadomość w zakresie obowiązujących w tym obszarze regulacji, a także niebezpieczeństw, jakie w przypadku
ich nieprzestrzegania mogą grozić osobom, których dane dotyczą.

Jest to duży problem, ponieważ aby instrumenty ochrony danych osobowych były rzeczywiście skuteczne, wymagają one systemowego i wielowymiarowego podejścia. Często może je zagwarantować wyłącznie inicjatywa posiadająca poparcie najwyższego kierownictwa organizacji.

Konsekwencje, których można uniknąć

W 2023 r. do Prezesa UODO wpłynęło ponad 14 tysięcy zgłoszeń naruszeń ochrony danych osobowych, czyli naruszeń bezpieczeństwa rodzących ryzyko wystąpienia negatywnych skutków dla osób fizycznych[1] . Wśród najczęstszych przyczyn takich zdarzeń można wymienić m.in.

- błędy pracowników,
- nieznajomość lub brak stosownych procedur i polityk ochrony danych
- oraz nieodpowiednie zabezpieczenia techniczne.

Administratorzy nie byli w stanie zapobiec wszystkim odnotowanym incydentom, jednakże w przypadku większości z nich dało się uniknąć albo przynajmniej znacznie ograniczyć konsekwencje dla osób, których dane przetwarzano. W tym kontekście fundamentalne znaczenie mają przemyślane i proporcjonalne inwestycje w ochronę danych osobowych oraz skuteczne mechanizmy zaradcze. Tymczasem niechęć kierownictwa wielu organizacji do akceptacji dodatkowych wydatków sprzyja urzeczywistnianiu się ryzyka w sytuacjach, w których można się przed nim uchronić.

Pozorna oszczędność

Pamiętajmy zatem, że przedkładanie korzyści biznesowych ponad bezpieczeństwo również może kosztować.

Najlepszym tego dowodem jest wyposażenie organów nadzorczych, takich jak Prezes UODO, w możliwość nakładania administracyjnych kar pieniężnych w przypadku naruszania przepisów RODO. Te zaś mogą sięgać nawet wielu milionów euro. Co więcej, osobom, które ponoszą szkody w wyniku takich naruszeń, przysługuje prawo do uzyskania odszkodowania.

Nie trzeba jednak powoływać się na argument sankcji administracyjnych, aby uzasadnić, jak pozorna i krótkowzroczna może się okazać tego rodzaju oszczędność.

Według raportu CERT Polska w ubiegłym roku zarejestrowano przeszło 80 tysięcy unikalnych incydentów cyberbezpieczeństwa. To ponad stuprocentowy przyrost w stosunku do 2022 r. Co więcej, same ataki typu ransomware liczy się już na całym świecie w setkach milionów. Objęte nimi systemy informatyczne gromadzą nie tylko dane osobowe, ale także inne cenne i wrażliwe aktywa administratorów.

Przykłady te pokazują, że adekwatne gwarancje bezpieczeństwa informacji, również tych dotyczących osób fizycznych, stały się po prostu niezbędne we współczesnym świecie gospodarki opartej na danych.

Rola inspektora ochrony danych

Przedsiębiorstwa i organy publiczne często wyznaczają konkretną osobę do realizacji zadań dotyczących przetwarzania danych osobowych. Nie zapominajmy natomiast, że to na administratorze, a nie na osobie działającej w jego imieniu, spoczywa ciężar odpowiedzialności
za prawidłowe wykonywanie przepisów RODO.

Niezwykle ważną częścią systemu ochrony danych osobowych są w tym kontekście inspektorzy ochrony danych.

Wśród ich głównych zadań można wskazać budowanie świadomości administratorów, a zatem przede wszystkim najwyższego kierownictwa, na temat spoczywających na nich obowiązków. Monitorują oni także przestrzeganie przepisów RODO wewnątrz organizacji oraz doradzają poszczególnym jednostkom w tym zakresie.

Powszechnym zjawiskiem jest jednak przypisywanie inspektorom nieadekwatnych, nadmiarowych funkcji. Prowadzi to do obarczania ich zadaniami, za których wykonanie w świetle RODO odpowiada wyłącznie administrator. Skutkuje to również niedopuszczalnymi sytuacjami, w których inspektorzy w rzeczywistości nadzorują sami siebie.

Niezrozumienie roli inspektora ochrony danych oraz uchylanie się przez kadrę kierowniczą od obowiązków wynikających z RODO może zatem przesądzić o zaistnieniu konfliktu interesów i naruszeniu przepisów. Niewłaściwą praktyką jest więc np. obarczanie inspektorów odpowiedzialnością za stwierdzanie, kwalifikowanie i zgłaszanie naruszeń ochrony danych osobowych czy też łączenie pracy inspektora ochrony danych z funkcją pełnomocnika administratora lub innym stanowiskiem, w ramach którego inspektor uczestniczy w podejmowaniu decyzji o celach i sposobach przetwarzania.

Perspektywa zmian
Pomimo niepokojących zjawisk warto też zauważyć, że proces budowania świadomości w zakresie przetwarzania i ochrony danych osobowych postępuje. Liczne inicjatywy Prezesa UODO, niezwykle ważna aktywność inspektorów ochrony danych oraz całego środowiska osób zajmujących się tą tematyką, a także generalny wzrost zainteresowania cyberbezpieczeństwem wynikający z upowszechniania się rozmaitych technologii cyfrowych pozwalają żywić nadzieję na większe zaangażowanie decydentów w realizację zadań wynikających z RODO.

Należy również wspomnieć o wielu zakończonych niedawno oraz toczących się jeszcze na szczeblu unijnym procesach legislacyjnych, których efektem będzie rozbudowa całokształtu regulacji dotyczących przetwarzania danych, a także podniesienie rangi przepisów

obejmujących szeroko pojęte sprawy bezpieczeństwa cyfrowego.

Niezależnie od tego w najbliższych miesiącach i latach wciąż pozostaje jeszcze wiele do zrobienia w kierunku podniesienia jakości zarządzania naszymi danymi osobowymi oraz zwiększenia poziomu ich bezpieczeństwa.

[1] Więcej na temat definicji „naruszenia ochrony danych osobowych” w „Biuletynie UODO” nr 1/03/23 na str. 13-14.