Warszawa, dn. 07.02.2023 r.

Rejestr naruszeń a kontrola Prezesa Urzędu Ochrony Danych Osobowych

Od ponad czterech lat, kiedy obowiązuje ogólne rozporządzenie o ochronie danych, wiele mówi się o naruszeniach ochrony danych osobowych. Zarówno na blogu iSecure jak i innych portalach, znaleźć można nałożone na administratorów danych szczególne obowiązki związane z dokonaniem zgłoszenia naruszeń ochrony danych Prezesowi Urzędu Ochrony Danych Osobowych, a także wymogu prowadzenia dokumentacji naruszeń. Pisaliśmy o tym, kiedy mamy do czynienia z naruszeniem, jak należy dokonać zgłoszenia naruszenia oraz w jaki sposób zawiadomić osoby fizyczne.

Praktyka pokazuje, że liczba zgłoszeń stale rośnie. A więc rośnie również świadomość organizacji w związku z pojawieniem się naruszenia. Poniższy tekst poświęcę prowadzenia rejestru naruszenia – o tym niewiele się mówi, a pamiętajmy, iż RODO wymaga od nas pełnej rozliczalności. Istotne jest, aby organ kontrolny, w tym wypadku Prezes Urzędu Ochrony Danych Osobowych, mógł zweryfikować, czy administrator dysponował odpowiednią dokumentacją.

Prezes UODO wskazał określone dokumenty jako must have każdego administratora. Wśród tych dokumentów znajduje się przede wszystkim, dokumentacja dotycząca naruszeń. Podkreślam to, gdyż w przypadku kontroli, w pierwszej kolejności będzie zwracana uwaga właśnie na tę dokumentację.

Obowiązek prowadzenia rejestru naruszeń

Zgodnie z wymaganiami art. 33 ust. 5 RODO administrator musi rejestrować informacje o naruszeniu obejmujące okoliczności naruszenia ochrony danych osobowych, przebieg i naruszone dane osobowe.

Co powinno się znaleźć we wskazanym rejestrze naruszeń?

Odnośnie do zakresu rejestru, wskazówki znajdziemy w wytycznych Grupy Roboczej w art. 29 nr WP 250: Zgodnie z nimi: „Chociaż administrator określa metody i strukturę dokumentowania naruszeń, we wszystkich przypadkach należy uwzględnić określone kluczowe elementy zapisywanych informacji. Zgodnie z art. 33 ust. 5 administrator jest zobowiązany do rejestrowania szczegółowych informacji na temat naruszenia, które obejmują jego przyczyny, przebieg wydarzeń oraz zakres danych osobowych, których dotyczyło naruszenie. Powinny one obejmować również skutki i konsekwencje naruszenia, uwzględniając działania zaradcze podjęte przez administratora".

Z mojego punktu widzenia, patrząc na powyższe wytyczne i praktykę, w rejestrze należy ująć:

- informacje o wystąpieniu zdarzenia i stwierdzeniu naruszenia (data i miejsce zdarzenia, data i źródło uzyskania informacji, data i godzina stwierdzenia naruszenia);
- okoliczności naruszenia (charakter naruszenia, kategoria osób, zakres danych, liczba osób, których naruszenie dotyczy);
- skutki naruszenia (opis kategorii naruszenia);
- środki naprawcze i zaradcze;

- czy zgłoszono naruszenie do PUODO – data zgłoszenia, jeżeli nie to z jakich powodów;
- czy poinformowano osoby, których dane dotyczą, jeśli tak, to w jaki sposób, jeśli nie, to dlaczego;
- rola w naruszeniu (Administrator czy Procesor);
- konsekwencje naruszenia.

W rejestrze zatem powinny znaleźć się zarówno naruszenia ochrony danych osobowych podlegające obowiązkowi notyfikacyjnemu Prezesowi UODO, jak i te, które nie podlegają zgłoszeniu organowi nadzorczemu ze względu na to, że mało prawdopodobne jest, by skutkowały one ryzykiem naruszenia praw lub wolności osób fizycznych.
Ewidencja powinna obejmować ponadto skutki i konsekwencje naruszenia oraz działania naprawcze podjęte przez administratora. Prowadzenie ewidencji łączy się z zasadą rozliczalności przewidzianą w art. 5 ust. 2 RODO oraz obowiązkami administratora wynikającymi z art. 24 RODO.

Jak wskazuje art. 33 ust. 5 RODO, organ nadzorczy może zażądać dostępu do dokumentacji (ewidencji) naruszeń i dokumentacja ta powinna pozwolić organowi na weryfikowanie przestrzegania RODO w zakresie tych obowiązków. Brak udokumentowania naruszenia we właściwy sposób może prowadzić do wykonania przez organ nadzorczy uprawnień na mocy art. 58 RODO lub nałożenia administracyjnej kary pieniężnej zgodnie z art. 83 RODO
Art. 33 ust. 5 RODO, który stanowi o wymogu dokumentowania naruszeń ochrony danych, nie wskazuje szczególnej formy, w jakiej rejestr naruszeń ma być prowadzony. Najbardziej praktycznym rozwiązaniem, który rekomenduje się przy wdrożeniu RODO pozostaje prowadzenie rejestru w formie elektronicznej w taki sposób, który umożliwi łatwą aktualizację dokumentu oraz ewentualne jego przesłanie/wydrukowanie przedstawicielom organu nadzorczego.

Pamiętajmy, że nie tylko na administratorze danych, ale również na podmiocie przetwarzającym ciąży obowiązek dokumentowania naruszenia przetwarzania danych osobowych.

Rejestr powinien również służyć możliwości monitorowania czy podmiot dokonuje odpowiednich zawiadomień o naruszeniach. Wszystkie obowiązki związane z zasadą rozliczalności, a tym samym z dokumentowaniem naruszeń zostały wskazane w art. 33-34 RODO oraz w motywach 85-87.

Olga Skotnicka – partner, specjalista ds. ochrony danych osobowych