# Procedura postępowania w przypadku naruszenia ochrony danych osobowych

Od 25 maja 2018 r. administrator ochrony danych ma obowiązek zgłaszania wszelkich naruszeń bezpieczeństwa danych osobowych w czasie do 72 godzin od naruszenia, bezpośrednio do właściwego organu nadzoru – Prezesa UODO (art. 33 RODO). Poznaj wewnętrzne elementy postępowania w przypadku naruszenia danych osobowych.

**Krok 1.** Określenie, jakie zdarzenia mogą stanowić naruszenia ochrony danych osobowych, przy uwzględnieniu specyfiki danego administratora (na podstawie definicji naruszenia ochrony danych).

**Krok 2.** Sposób reagowania na naruszenia przez pracowników, którzy je ujawnili. Powinien się tu znaleźć:

- obowiązek niezwłocznego poinformowania o zdarzeniu osoby nadzorującej (powinien to być inspektor ochrony danych),
- obowiązek pozostawienia miejsca zdarzenia w stanie nienaruszonym do czasu przybycia inspektora ochrony danych.

**Krok 3.** Obowiązki inspektora ochrony danych związane z dokumentowaniem okoliczności naruszenia, tj.:

- sporządzenie notatki z przeprowadzonych oględzin miejsca zdarzenia,
- sporządzenie kopii obrazu wyświetlonego na ekranie monitora komputera związanego z naruszeniem,
- sporządzenie kopii zapisów rejestrów systemu informatycznego służącego do przetwarzania danych lub zapisów konfiguracji technicznych środków zabezpieczeń systemu,
- odebranie pisemnych wyjaśnień od osoby, która ujawniła naruszenie.

**Krok 4.** Obowiązek niezwłocznego przedstawienia zebranych materiałów administratorowi danych, który z pomocą inspektora ochrony danych, w terminie i na podstawie przesłanek określonych w ogólnym rozporządzeniu o ochronie danych powinien ocenić, czy zaistniałe naruszenie podlega obowiązkowi zgłoszenia organowi nadzorczemu

**Krok 5.** Obowiązek przedstawienia administratorowi przez inspektora ochrony danych skutków naruszenia oraz środków i działań mających zaradzić naruszeniu, a także, jeżeli to konieczne, mających zminimalizować negatywne skutki naruszenia.

**Krok 6.** Jeżeli istnieje taki obowiązek – sporządzenie zgłoszenia do organu nadzorczego oraz zamieszczeniu informacji naruszeniu na stronie ww lub BIP jednostki.

**Krok 7.** Udokumentowanie skutków oraz podjętych środków i działań, o których mowa w pkt5

- Ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn.: Dz.U. z 2016 r. poz. 922).
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.Urz. UE. L nr 119, str. 1) - punkt 83, 97 preambuły, art. 24, art. 28, art. 32–39.