Procedura postępowania w sprawach naruszenia danych osobowych

Stwierdzenie lub podejrzenie, że doszło do naruszenia danych osobowych

Pracownik informuje o tym fakcie bezpośredniego przełożonego.

Przełożony zgłasza ten fakt Inspektorowi Ochrony Danych na specjalnym formularzu albo na pomocną platformy **ado.usz.edu.pl.**

Inspektor Ochrony Danych zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości i ciągłości pracy, odbiera dokładną relację i dokumentację, dokonuje oceny ryzyka naruszenia praw i wolności osób fizycznych oraz kwalifikuje zdarzenie, jako incydent albo naruszenie. Jeżeli zachodzi taka potrzeba przy dokonaniu oceny ryzyka nawiązuje kontakt ze specjalistami zewnętrznymi.

Inspektor Ochrony Danych sporządza raport.

Inspektor Ochrony Danych proponuje działania naprawcze.

W przypadku stwierdzenia naruszenia ochrony danych osobowych administrator bez zbędnej zwłoki zgłasza je Prezesowi Urzędu Ochrony Danych Osobowych.

Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

Pracownik podejmuje czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz zabezpieczenia dowodów umożliwiające ustalenie przyczyn oraz skutków naruszenia

Pracownik powinien zaniechać działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Inspektora Ochrony Danych lub innej osoby upoważnionej przez Administratora danych.

Typowe sytuacje, gdy pracownik powinien powiadomić przełożonego:

- ślady na drzwiach, oknach i szafach wskazują na próbę włamania;
- dokumentacja jest niszczona bez użycia niszczarki;
- fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie;
- otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe;
- niewylogowanie się przed opuszczeniem stanowiska pracy;
- pozostawienie danych w drukarce, na ksero;
- niezamknięcie pomieszczenia z komputerem;
- niewykonanie w określonym terminie kopii bezpieczeństwa;
- prace na informacjach służbowych w celach prywatnych;
- ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe;
- wynoszenie danych osobowych w wersji papierowej lub elektronicznej na zewnątrz firmy bez upoważnienia;
- udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej lub ustnej;
- stwierdzenie próby modyfikacji danych lub zmian w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);
- telefoniczne próby wyłudzenia danych osobowych;
- kradzież komputera lub twardego dysku z danymi osobowymi;
- utrata kontroli nad kopią danych osobowych;
- maile zachęcające do ujawnienia identyfikatora lub hasła;
- pojawienie się szkodliwego oprogramowania (wirusy, robaki, malware) lub niestandardowe zachowanie komputerów;
- istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki";
- hasła do systemów przechowywane są w pobliżu komputera.