

Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych

§ 1

Osoby zobowiązane do ochrony danych osobowych

1. Osobami odpowiedzialnymi za ochronę danych osobowych, zgodnie z właściwością, są :
 - a) Starosta
 - b) IOD,
 - c) ASI,
 - d) KKO,
 - e) osoby upoważnione do przetwarzania danych osobowych,
 - f) osoby, które nie przetwarzają danych osobowych, ale w ramach czynności poznały sposoby ich zabezpieczania.

§ 2

Obowiązki osób zobowiązanych do ochrony danych osobowych w sytuacji naruszenia ochrony danych osobowych

1. Każdy zobowiązany do ochrony danych osobowych, zwany dalej Zobowiązany, jeśli stwierdzi lub podejrzewa naruszenie zabezpieczenia danych osobowych, powinien niezwłocznie poinformować o tym:
 - a) właściwego KKO, którego obowiązkiem jest poinformowanie o naruszeniu Administratora lub osoby zastępującej Starostę i IOD.
 - b) bezpośrednio Administratora w sytuacjach szczególnych, do których zaliczyć można podejrzenie braku bezstronności osób wskazanych w § 2 pkt. 1 lit. a).
2. Informację o naruszeniu Administrator powinien niezwłocznie przekazać do IOD w celu umożliwienia mu realizacji jego obowiązków.
3. Zobowiązany, który stwierdził lub podejrzewa naruszenie zabezpieczenia danych osobowych, oprócz obowiązku wymienionego w § 2 pkt. 1 powinien:
 - a) powstrzymać się od wykonywania pracy lub jakichkolwiek czynności mogących spowodować zatarcie śladów lub dowodów naruszenia,
 - b) podjąć, odpowiednie do zaistniałej sytuacji działania niezbędne do zapobieżenia dalszym zagrożeniom, które mogą skutkować naruszeniem danych osobowych.

3. Administrator, a w przypadku jego nieobecności osoba wyznaczona przez Starostę, po stwierdzeniu lub uzyskaniu informacji o naruszeniu ochrony danych osobowych powinien:
 - b) przystąpić do identyfikacji rodzaju zdarzenia, a w szczególności do określenia skali zniszczeń, dostępu do danych osobowych itp.,
 - c) podjąć odpowiednie kroki w celu zminimalizowania szkód i rozmiarów zdarzenia oraz zabezpieczenia przed usunięciem śladów zdarzenia,
 - d) osobiście lub polecić IOD w terminie 72 godzin przesłać do właściwego Organu Nadzorczego zgłoszenie naruszenia ochrony danych osobowych jeżeli skutkowało ono ryzykiem naruszenia praw i wolności osób fizycznych;
 - e) osobiście lub polecić IOD bez zbędnej zwłoki zawiadomić osobę, której dane dotyczą o naruszeniu jeżeli skutkowało ono ryzykiem naruszenia praw i wolności osób fizycznych; postępowanie to powinno być zgodne z art. 34 RODO,
4. IOD jest zobowiązany zarejestrować zdarzenie; wzór „Rejestru naruszeń ochrony danych osobowych w Starostwie Powiatowym w Nowym Tomyślu” stanowi załącznik nr 1 do tej Instrukcji,
5. Administrator, czynności o których mowa w § 2 pkt. 3 lit. b), c), w sytuacjach szczególnych, takich jak konieczność zgłoszenia naruszenia ochrony danych osobowych do właściwego Organu Nadzorczego, może dokumentować wykorzystując dokumenty określone w rozdziale XIV Polityki „Monitorowanie przestrzegania RODO, innych właściwych przepisów o ochronie danych osobowych oraz PODO”; sporządzeniem tej dokumentacji powinien zająć się wskazany pracownik Administratora, a w sytuacjach szczególnych IOD; sprawozdanie z okoliczności zdarzenia osoba sporządzająca przedkłada Staroście.
6. W przypadku zdarzenia mającego związek z systemem informatycznym ASI zobowiązany jest do:
 - a) szczegółowej analizy systemu w celu potwierdzenia lub wykluczenia faktu naruszenia,
 - b) wygenerowania, wydrukowania wszystkich możliwych dokumentów, raportów lub zestawień, które mogą pomóc w ustaleniu okoliczności zdarzenia, opatrując je
 - c) datą i podpisem,
 - d) fizycznego odłączenia urządzenia, segmentu sieci, które mogły umożliwić dostęp do bazy danych osobowych osobie nieupoważnionej,
 - e) wylogowania użytkownika podejrzanego o naruszenie ochrony danych osobowych,
 - f) zmiany haseł na konta, poprzez które uzyskano nielegalny dostęp,
 - g) przywrócenia normalnego działania systemu, przy czym, jeżeli nastąpiło uszkodzenie bazy danych, przywrócenia jej z ostatniej kopii awaryjnej z zachowaniem środków ostrożności przed ponownym dostępem tą samą drogą przez osobę nieupoważnioną,

5. ASI o podjętych działaniach powinien niezwłocznie poinformować Administratora.
6. Wszyscy zobowiązani mają obowiązek udzielić wszelkiej niezbędnej pomocy przy realizacji zadań przez IOD.