Naruszenia ochrony danych

Uniwersytet Gdański / Akademia Marynarki Wojennej

linkedin.com/in/piotr-siemieniak/

Wprowadzenie

- Źródła prawa dotyczące naruszeń ochrony danych
- Naruszenia ochronie danych w ogólnym rozporządzeniu o ochronie danych
- Przykłady naruszeń ochrony danych
- Podsumowanie

Źródła prawa

- Dyrektywa 97/66/WE w sprawie przetwarzania danych osobowych i ochrony prywatnych danych w sektorze telekomunikacyjnym (uchylony)
- Dyrektywa 2002/58/WE o prywatności i łączności elektronicznej, która zastępuje Dyrektywę 97/66/WE (obowiązujący)
- Rozporządzenie Komisji (UE) NR 611/2013 w sprawie środków mających zastosowanie przy powiadamianiu o przypadkach naruszenia danych osobowych, na mocy dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady o prywatności i łączności elektronicznej (obowiązujący)

Źródła prawa

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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 (ogólne rozporządzenie o ochronie danych) (obowiązujący, stosowany od 25 maja 2018 r.)
- Ustawa o krajowym systemie cyberbezpieczeństwa (projekt)

Obowiązek notyfikacji naruszeń w ustawie prawo telekomunikacyjne

- Zmiany, które wprowadziły obowiązek notyfikacyjny obowiązują od dnia 22 marca 2013 r.
- Dostawca publicznie dostępnych publicznie usług informuje GIODO o naruszeniu
- Zawiadomienie o naruszeniu musi zostać dokonane niezwłocznie, lecz nie później niż 3 dni od stwierdzenia naruszenia
- Dostawca publicznie dostępnych usług prowadzi rejestr naruszeń

Definicja naruszenia ochrony danych

„naruszenie ochrony danych osobowych” oznacza **naruszenie bezpieczeństwa** prowadzące do **przypadkowego lub niezgodnego z prawem** zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

Przykłady naruszeń ochrony danych

- Skradziony służbowy laptop pracownika działu handlowego.
  - Czy kradzież laptopa może wiązać się z naruszeniem ochrony danych?
- Luka bezpieczeństwa istniejąca w oprogramowaniu, która została wykorzystana do wykradzenia informacji zapisanych w bazie danych tego oprogramowania (np. zainstalowana nieaktualna wtyczka do Wordpress).
  - Czy nieaktualne oprogramowanie może wiązać się z naruszeniem ochrony danych?
- Pracownik dla swojej wygody przesyłał dane klientów na swoją skrzynkę pocztową.
  - Czy w momencie zakończenia stosunku pracy dochodzi do naruszenia ochrony danych?

Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu (rodo art. 33)

1. **[TERMIN I WARUNKI ZGŁOSZENIA]** W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, **nie później niż w terminie 72 godzin po stwierdzeniu naruszenia** – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. **Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia**.
2. **[INFORMOAWNIE ADO O NARUSZENIU]** Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych **bez zbędnej zwłoki zgłasza je administratorowi**.

Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu (rodo art. 33)

3. Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:

a) opisywać **charakter naruszenia** ochrony danych osobowych, w tym w miarę możliwości **wskazywać kategorie i przybliżoną liczbę osób**, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;

b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;

c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;

d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Przykładowe konsekwencje naruszenia

Sklep internetowy sprzedający wiertarki

- Kradzież tożsamości
- Spam

Strona serwisu towarzyskiego

- Kradzież tożsamości
- Spam
- Dyskryminacja
- Wykluczenie społeczne
- Utrata pracy

Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu (rodo art. 33)

4. [SUKCESYWNE UZUPEŁNIANIE INFORMACJI] Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki
5. [DOKUMENTOWANIE NARUSZEŃ OCHRONY DANYCH] Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.

Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych (rodo art. 34)

1. **[WARUNEK ZAWIADOMIENIA O NARUSZENIU]** 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.
2. **[CHARAKTERYSTYKA ZAWIADOMIENIA]** Zawiadomienie, o którym mowa w ust. 1 niniejszego artykułu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art. **33 ust. 3 lit. b), c) i d).**

Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych (rodo art. 34)

3. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:

a) **[WDROŻENIE ŚRODKÓW] administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony** i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

b) **[MITYGACJA RYZYKA] administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby**, której dane dotyczą, o którym mowa w ust. 1;

c) **[NIEWSPÓŁMIERNY WYSIŁEK] wymagałoby ono niewspółmiernie dużego wysiłku**. W takim przypadku wydany zostaje **publiczny komunikat lub zastosowany zostaje podobny środek**, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

Wymogi dokumentacyjne przy naruszeniach

- Wynikają z art. 33 ust. 5:
  [DOKUMENTOWANIE NARUSZEŃ OCHRONY DANYCH] Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.
- Wynikają z art. 33 ust. 3:

a) opisywać **charakter naruszenia** ochrony danych osobowych, w tym w miarę możliwości **wskazywać kategorie i przybliżoną liczbę osób**, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;

b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;

c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;

d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Podsumowanie

- [TERMIN] Prawnie ustanowiony termin 72 godzin na zgłoszenie naruszenia ochrony danych jest niezwykle krótki.
- Język zgłoszenia
- [TRENING] Zgłaszanie naruszeń ODO regularnych ćwiczeń, np. jak ćwiczenia PPOŻ.
- [ADO / PROCESOR] Należy pomyśleć o dedykowanym środku komunikacji, gdzie każdy może zgłosić naruszenie lub podejrzenie naruszenia ochrony danych (odrębnym od adresu IOD).
- [ŹRÓDŁO] Zgłaszanie naruszeń ochrony danych bazuje na przepisach prawa telekomunikacyjnego, gdzie wymóg prawny funkcjonuje od wielu lat.
- [JĘZYK] Zgłoszenie naruszenia musi być wykonane w języku

Dziękuję za uwagę

Uniwersytet Gdański / Akademia Marynarki Wojennej

linkedin.com/in/piotr-siemieniak/