

Naruszenie danych 12 punktów na początek

Dla osoby koordynującej reakcję w gabinecie lub placówce medycznej.

ZAZNACZ PO SPRAWDZENIU - PYTANIA, NIE GOTOWE ODPOWIEDZI

- ☐ **01 Zdarzenie i czas**
Co się stało, kiedy to wykryto i od kiedy administrator wie o naruszeniu?
-
- ☐ **02 Ograniczenie skutków**
Czy zatrzymano dalszy dostęp lub ujawnienie bez niszczenia dowodów?
-
- ☐ **03 Osoba odpowiedzialna**
Kto koordynuje działania i czy zawiadomiono IOD lub właściwy zespół?
-
- ☐ **04 Systemy i nośniki**
Jakie systemy, konta, urządzenia i kanały komunikacji obejmuje zdarzenie?
-
- ☐ **05 Kategorie danych**
Czy dotyczą danych o zdrowiu, identyfikacyjnych lub innych wrażliwych informacji?
-
- ☐ **06 Skala**
Ilu osób i jakich rekordów może dotyczyć naruszenie?
-

Naruszenie danych / ciąg dalszy

Zaznacz tylko te punkty, które rzeczywiście zostały sprawdzone.

- ☐ **07 Dowody**
Czy zabezpieczono logi, wiadomości, kopie i chronologię bez niepotrzebnego kopiowania danych?
- ☐ **08 Role stron**
Kto jest administratorem, a kto podmiotem przetwarzającym i jakie ma obowiązki?
- ☐ **09 Ocena ryzyka**
Jakie skutki dla praw i wolności osób mogą wystąpić; co ogranicza ryzyko?
- ☐ **10 Zgłoszenie do UODO**
Czy wymagane jest zgłoszenie; jeśli tak, jak dotrzymać terminu liczonego od stwierdzenia?
- ☐ **11 Zawiadomienie osób**
Czy wysokie ryzyko wymaga poinformowania osób, których dane dotyczą?
- ☐ **12 Rejestr i naprawa**
Czy udokumentowano decyzję, działania naprawcze i plan zapobiegania powtórzeniu?

KIEDY ZATRZYMAĆ SIĘ I WYJAŚNIĆ?

Nie każde naruszenie wymaga zgłoszenia, lecz każde wymaga oceny i dokumentacji. Gdy zgłoszenie jest konieczne, RODO przewiduje działanie bez zbędnej zwłoki - w miarę możliwości nie później niż 72 godziny od stwierdzenia.

ŹRÓDŁA DO WERYFIKACJI

- UODO - zgłaszanie naruszeń
- RODO - art. 33 i 34