

# **Procedura postępowania w sytuacji naruszenia danych**

## **w Zespole Szkół Chemiczno- Elektronicznych im. Jana Pawła II w Inowrocławiu**

**aktualizacja: kwiecień 2022**

### **Cele ustalania zasad postępowania w sytuacji naruszenia:**

- a. RODO nakazuje, aby wszelkie przypadki naruszenia praw lub wolności osób były rejestrowane i stanowiły podstawę ponownej analizy ryzyka związanego z przetwarzaniem;
  - b. Ponadto, część naruszeń, a konkretnie te, które z wysokim prawdopodobieństwem mogą spowodować naruszenie praw lub wolności osób (wyrządzić krzywdę lub szkodę) podlegają zgłoszeniu do Prezesa Urzędu Ochrony Danych Osobowych w **nieprzekraczalnym terminie 72 godzin od momentu powzięcia informacji o tym naruszeniu;**
1. Niniejsza procedura służy usprawnieniu obsługi incydentów i umożliwieniu realizacji ww. obowiązków. W sytuacji gdy do Zespołu Szkół Chemiczno-Elektronicznych uczęszczają uczniowie posiadający Status uchodźcy z kraju objętego wojną (z Ukrainy) niewładający biegle językiem polskim, albo w ogóle nieporozumiewający się w tym języku, niniejsza procedura nabiera szczególnej ważności.
  2. Generalne zasady postępowania w sytuacji naruszenia:
    - a. Niewłaściwa obsługa naruszenia stanowi typ działania, które jest karane z najwyższą surowością. Dlatego:
      - i. nie należy bagatelizować nawet drobnych naruszeń, dotyczących niewielkiej ilości danych lub danych powszechnie dostępnych kategorii - procedura powinna być realizowana za każdym razem identycznie;
      - ii. wszelkie naruszenia należy odnotowywać w wewnętrznym rejestrze naruszeń – załącznik do niniejszej procedury w arkuszu kalkulacyjnym
    - b. W celu uniknięcia sytuacji, w której istotne informacje nie zostaną udokumentowane, jak również sytuacji, w której z jakiegokolwiek przyczyny, istotne informacje nie zostaną ustalone, wszelkie naruszenia opracowuje się na podstawie wzoru zgłoszenia naruszenia udostępnionego przez Urząd Ochrony Danych Osobowych na stronie PUODO;
      - i. osoba stwierdzająca naruszenie powinna niezwłocznie wydrukować wzór zgłoszenia i zacząć go wypełniać zaczynając od części 3;
      - ii. w przypadku potrzeby przekazania obsługi naruszenia innej osobie, należy jej przekazać częściowo wypełniony wzór zgłoszenia;
    - c. W przypadku ustalenia, że niektórych informacji wymaganych do wypełnienia zgłoszenia nie da się ustalić albo może to zająć więcej niż 8 godzin, należy dokonać zgłoszenia (do Urzędu lub do Administratora) bez tych danych i uzupełnić je, o ile zajdzie taka możliwość, w terminie późniejszym.

3. Kwalifikacja naruszenia (rozpoznanie, czy naruszenie może z dużym prawdopodobieństwem naruszyć prawa lub wolności osób fizycznych):

- a. Naruszenia, które mogą z dużym prawdopodobieństwem, naruszyć prawa lub wolności osób fizycznych, podlegają zgłoszeniu do Urzędu Ochrony Danych Osobowych;
- b. Kwalifikacji naruszenia powinien dokonywać wyłącznie Administrator Danych Osobowych;
- c. W przypadku naruszeń na danych powierzonych do przetwarzania (administrowanych przez kontrahenta), zasadne jest pozostawienie tej decyzji Administratorowi Danych Osobowych;

4. W celu właściwej kwalifikacji naruszenia, warto zadać sobie następujące pytania: Czy istnieje ryzyko, że naruszenie wystąpiło wielokrotnie, a zaistniałe okoliczności stanowią wyłącznie pierwszy przypadek jego wykrycia? Czy istnieje realne ryzyko, że naruszenie to będzie się powtarzać w przyszłości (np. stosowane do tej pory zabezpieczenia okazały się niedostateczne)? Czy są powody domniemywać, że naruszenie stanowi rezultat świadomego działania, obliczonego na kradzież lub zniszczenie danych osobowych? Czy naruszenie wiąże się z utratą lub ujawnieniem informacji istotnych z perspektywy prywatności i bezpieczeństwa osób (przykładowo: dane dotyczące jakości pracy, dane dotyczące sytuacji finansowej, rodzinnej lub zdrowotnej, dane dotyczące naruszeń prawa, dane dotyczące orientacji seksualnej, inne dane, o których wiadomo, że pozwalają przedstawić osobę, której dotyczą w sposób dyskredytujący, kopie dokumentów tożsamości, treść pism urzędowych, sądowych lub komorniczych itd.)? Czy naruszenie wiąże się z utratą lub ujawnieniem danych dotyczących więcej niż 1 osoby? Czy skutki naruszenia są nieodwracalne (np. danych nie da się odzyskać z kopii bezpieczeństwa lub czy osoba, która je przypadkiem otrzymała nie jest na tyle wiarygodna, aby można zasadnie uznać, że wezwanie jej do usunięcia danych będzie skuteczne)? Czy naruszenie dotyczy danych osób, które z zasady dysponują ograniczoną zdolnością do ochrony i dochodzenia swoich praw, takich jak osoby niepełnosprawne, dzieci, obcokrajowcy, uchodźcy (uczniowie i ich opiekunowie prawni) z Ukrainy, niewładający biegle językiem urzędowym? Czy naruszenie już doprowadziło do pogwałcenia praw osoby (np. doszło do pomówienia, dyskryminacji, kradzieży tożsamości, środków z konta bankowego, nieuzasadnionej utraty wiarygodności, traumy, itd.)?

5. Jeżeli odpowiedź na którekolwiek z powyższych pytań jest twierdząca, naruszenie należy zakwalifikować jako naruszające z wysokim prawdopodobieństwem prawa lub wolności osób. Jeżeli odpowiedzi na wszystkie powyższe pytania są negatywne, prawdopodobnie naruszenie nie stwarza wysokiego ryzyka jednak ostateczną decyzję w tym obszarze podejmuje zawsze i na swoją wyłączną odpowiedzialność Administrator Danych Osobowych.

6. Kroki podejmowane w toku obsługi naruszenia:

- a. Z chwilą powzięcia informacji o naruszeniu, osoba, która się o nim dowiedziała, wykonuje poniższe kroki w kolejności, w jakiej zostały opisane:
- b. Zawiadamia ADO i IOD;
- c. Drukuje wzór zgłoszenia naruszenia – formularz interaktywny stanowiący załącznik do niniejszej procedury;
- d. W oparciu o wiedzę własną oraz dokonując wszelkich rozsądnych starań w celu zdobycia dodatkowych informacji, uzupełnia wzór zgłoszenia naruszenia zaczynając od części 3 (Czas naruszenia);
- e. Z chwilą wyczerpania dalszych możliwości gromadzenia wiedzy lub na wyraźne polecenie ADO, osoba ta przekazuje częściowo wypełniony wzór zgłoszenia osobie wskazanej przez ADO;
- f. Ewentualna osoba dokonująca uzupełnienia wzoru zgłoszenia na polecenie ADO również wykonuje czynności wskazane powyżej.
- g. Z chwilą otrzymania wzoru zgłoszenia, ADO podejmuje decyzję o kwalifikacji naruszenia lub (w przypadku naruszenia na danych stanowiących przedmiot powierzenia) zawiadamia kontrahenta będącego Administratorem danych pozostawiając mu swobodę decyzyjną w zakresie kwalifikacji naruszenia;
- h. W przypadku stwierdzenia, że naruszenie może z wysokim prawdopodobieństwem zagrażać prawom lub wolnościom osób, ADO dokonuje zawiadomienia Urzędu Ochrony Danych Osobowych zgodnie z procedurą wskazaną na stronie Urzędu: <https://uodo.gov.pl/pl/134/233>, a ze wzorem zgłoszenia postępuje tak, jak gdyby naruszenie nie stwarzało wysokiego ryzyka (czyli w sposób opisany poniżej);
- i. W przypadku zakwalifikowania naruszenia jako niegenerującego wysokiego ryzyka, ADO archiwizuje wzór zgłoszenia nie dokonując zgłoszenia;
- j. Zarchiwizowane wzory zgłoszeń stanowią wewnętrzny rejestr naruszeń i są przechowywane dla celów dowodowych.

Załączniki:

1. Formularz zgłoszenia naruszenia do PUDO,
2. Rejestr naruszeń danych osobowych (wewnętrzny).