PROCEDURA POSTĘPOWANIA W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

I

1. Procedura opisana w niniejszym dokumencie określa sposób postępowania w Szkole Nr 8 w Gdyni (zwn. dalej Placówką) w przypadku stwierdzenia naruszenia ochrony danych osobowych.
2. Zgodnie z art. 4 pkt 12 RODO, naruszenie ochrony danych osobowych to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem:
    3. zniszczenia,
    4. utracenia,
    5. zmodyfikowania,
    6. nieuprawnionego ujawnienia lub
    7. nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
8. Każde naruszenie danych osobowych jest zdarzeniem zagrażającym bezpieczeństwu, ale nie każde zdarzenie zagrażające bezpieczeństwu stanowi naruszenie ochrony danych osobowych.
9. Pracownicy placówki oświatowej zobowiązani są zgłaszać każde zdarzenie zagrażające bezpieczeństwu, a ustalenie czy stanowi ono naruszenie ochrony danych osobowych należy do administratora.
10. Przykładowy wykaz naruszeń ochrony danych osobowych i podmiotu, które należy zawiadomić został określony w załączniku do Wytycznych Grupy Roboczej art. 29 *w sprawie powiadomień o naruszeniu ochrony danych osobowych na mocy rozporządzenia 2016/679, 03.10.2017 r.*

II

1. Naruszenia ochrony danych osobowych można zaklasyfikować ze względu na:
    2. naruszenie dostępności – niedozwolona lub przypadkowa utrata dostępu do danych osobowych lub zniszczenie ich (trwała utrata lub zniszczenie danych osobowych). Zdarzenie skutkujące utratą dostępności do danych osobowych przez pewien czas stanowi naruszenie ochrony danych osobowych i należy je udokumentować. *W zależności od okoliczności powiadomienie organu nadzorczego czy poszkodowanych osób może ale nie musi być wymagane* – należy to oceniać w zależności od konkretnych przypadków.

3. naruszenie integralności – niedozwolona lub przypadkowa zmiana danych osobowych.
4. W zależności od okoliczności naruszenie może dotyczyć jednocześnie poufności, dostępności i integralności danych osobowych lub dowolnej kombinacji tych kategorii.

III
Stwierdzenie zagrożenia bezpieczeństwa ochrony danych

1. Pracownik Placówki, który stwierdził lub podejrzewa fakt naruszenia bezpieczeństwa danych zobowiązany jest niezwłocznie zgłosić to Administratorowi Danych Osobowych (Dyrektorowi).
2. Dyrektor powiadamia o tym fakcie inspektora ochrony danych oraz administratora systemu informatycznego (jeśli naruszenie bezpieczeństwa dotyczy systemów informatycznych).
3. W związku ze zgłoszeniem powołuje się Zespół, w skład której wchodzą m.in.:
   4. inspektor ochrony danych – ewentualnie osoba sprawująca zastępstwo,
   5. administrator systemu informatycznego – ewentualnie osoba sprawująca zastępstwo,
   6. wyznaczony przez Administratora pracownik.
7. Jednocześnie należy przeprowadzić czynności zabezpieczające, których celem jest niedopuszczenie do powiększenia się skutków naruszenia ochrony danych osobowych. Jeżeli naruszenie ochrony danych osobowych dotyczy systemu informatycznego administrator systemu informatycznego podejmuje niezbędne działania zabezpieczające w porozumieniu z Dyrektorem i inspektorem ochrony danych. Jeżeli naruszenie ochrony danych związane jest z zabezpieczaniem fizycznym, wówczas Dyrektor w porozumieniu z inspektorem ochrony danych uzgadnia dalsze działania zabezpieczające.

IV
Stwierdzenie naruszenia ochrony danych osobowych

1. Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu (Prezesowi Urzędu Ochrony Danych Osobowych) musi być dokonane bez zbędnej zwłoki, nie później niż **w terminie 72 godzin po stwierdzeniu naruszenia**, chyba że jest mało

prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

2. Stwierdzenie naruszenia następuje w momencie, gdy Dyrektor ma wystarczający stopień pewności co do tego, że miało miejsce zdarzenie zagrażające bezpieczeństwu prowadzące do naruszenia bezpieczeństwa danych osobowych. Należy wypełnić Protokół stwierdzenia naruszenia ochrony danych osobowych.
3. W przypadku konieczności dokonania zgłoszenia naruszenia do organu nadzorczego,

   w zgłoszeniu należy co najmniej:

   4. opisać 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,
   5. podać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych,
   6. opisać możliwe konsekwencje naruszenia ochrony danych osobowych,
   7. opisać środki zastosowane lub proponowane w Placówce w celu ograniczenia negatywnych skutków naruszeniu ochrony danych osobowych,
   8. wskazówki postępowania dla osób, których dane naruszono, tak aby mogły zabezpieczyć się przed potencjalnymi negatywnymi skutkami naruszenia np.: prośba o zresetowanie hasła.

Jeżeli powyższych informacji, nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki:

- po dokonaniu pierwszego zgłoszenia można przekazywać na bieżąco organowi nadzorczemu aktualne informacje,
- w przypadku uzyskania w toku dochodzenia dowodów na to, że opanowano zdarzenie,

  a w rzeczywistości żadne naruszenie nie miało miejsca, informację tę można dodać do informacji już przekazanych do organu nadzorczego, a następnie zarejestrować zaistniałe zdarzenie jako takie niestanowiące naruszenia ochrony danych osobowych.

1. Do zgłoszenia (skonsultowanego uprzednio z inspektorem ochrony danych) przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia, aczkolwiek nie należy uznawać tej możliwości za rozwiązanie w trybie zwykłym.
2. Administrator danych dokumentuje sprawy z zakresu naruszeń prowadząc rejestr naruszeń, który zawiera:

3. datę zgłoszenia,
4. datę naruszenia jeżeli jest możliwa do określenia,
5. okoliczności naruszenia ochrony danych osobowych, jego skutki i konsekwencje,
6. podjęte działania naprawcze,
7. informacje o powiadomieniu organu nadzorczego, jeśli nie - konieczne jest uzasadnienie,
8. informacje o zawiadomieniu osób, których dane dotyczą, jeśli nie - konieczne jest uzasadnienie.

V
Zawiadamianie osoby, której dane dotyczą

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, bez zbędnej zwłoki zawiadamia się o tym osoby, których dane dotyczą.
2. Zawiadomienie należy przygotować jasnym i prostym językiem.
3. Należy bezpośrednio powiadomić osoby, których dane naruszono (e-mail, sms, bezpośrednia przesyłka pocztowa).
4. Przygotować wskazówki postępowania dla osób, których dane naruszono, tak aby mogły zabezpieczyć się przed potencjalnymi negatywnymi skutkami naruszenia np.: prośba o zresetowanie hasła.

VI
Zawiadomienie osoby, której dane dotyczą nie jest wymagane, gdy:

1. w Placówce wdrożono odpowiednie środki ochrony techniczne i organizacyjne,
   w szczególności takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do danych osobowych. Środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie,
2. w Placówce zastosowano następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
3. 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.

W przypadku braku powiadomienia osób, których dane naruszono należy wykazać przed organem nadzorczym, że został spełniony przynajmniej jeden z wyżej wymienionych warunków.

Jeżeli administrator nie zawiadomił jeszcze osób, których dane dotyczą, o naruszeniu ochrony danych osobowych, organ nadzorczy – biorąc pod uwagę prawdopodobieństwo, że to naruszenie ochrony danych osobowych spowoduje wysokie ryzyko – może tego od administratora zażądać lub może stwierdzić, że spełniony został jeden z warunków, o których mowa powyżej.

VII
Zadania podmiotu przetwarzającego w przypadku naruszenia ochrony danych

W przypadku powierzenia przetwarzania danych osobowych na podstawie art. 28 RODO należy zawrzeć postanowienie o zobowiązaniu podmiotu przetwarzającego do:

1. zgłaszania naruszenia ochrony danych osobowych administratorowi (bez zbędnej zwłoki, nie później niż w ciągu 24 godzin od jego stwierdzenia),
2. lub zgłoszenia naruszenia ochrony danych bezpośrednio do organu nadzorczego

   w imieniu administratora - konieczny jest odpowiedni zapis w umowie/porozumieniu oraz upoważnienie.

Uwaga: w obu przypadkach odpowiedzialność ciąży na administratorze.

Umowa/porozumienia w sprawie powierzenia przetwarzania danych osobowych muszą szczegółowo określać sposób realizacji tego obowiązku przez podmiot przetwarzający.

Link do strony PUODO: zgłoszenie naruszenia ochrony danych osobowych (formularze)

https://uodo.gov.pl/pl/134/233