SZKOŁA PODSTAWOWA Nr 2
im. Ks. Jana Twardowskiego
ul. Boh. Monte Cassino 25
15-873 Białystok
tel. 85 742 03 04
Reg. 000735227, NIP 542-20-73-403

Pieczęć Administratora

PROCEDURA OCENY POWAGI NARUSZENIA OCHRONY DANYCH OSOBOWYCH U ADMINISTRATORA

1. Celem procedury jest ocena poziomu naruszenia bezpieczeństwa danych osobowych (ich dostępności, poufności, integralności oraz rozliczalności) w celu zakwalifikowania zdarzenia wymagającego lub nie, zgłoszenia do Urzędu Ochrony Danych Osobowych i/lub poinformowania osób fizycznych, których dane dotyczą na temat zdarzenia, zgodnie z ciążącymi na administratorze obowiązkami określonymi w art. 33 i w art. 34 RODO.
2. Procedura została opracowana na podstawie rekomendacji Urzędu Ochrony Danych Osobowych i odnosi się do metodologii opublikowanej w dniu 30 maja 2019 w wytycznych pt. Obowiązki administratorów związane z naruszeniami ochrony danych osobowych, oraz metodologii oceny wagi naruszenia ochrony danych osobowych przygotowanej przez Agencję Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA).
3. Za przeprowadzenie oceny odpowiada Administrator/Inspektor Ochrony Danych
4. Niezależnie od wyniku oceny (od niskiego, do bardzo wysokiego) incydent ten zostaje odnotowany w prowadzonym przez administratora rejestrze incydentów.
5. Opis narzędzia oceny (miernika):

5.1. Jeżeli dane naruszenie powoduje:

- **Małe** prawdopodobieństwo ryzyka wystąpienia naruszenia praw lub wolności osób, których dane dotyczą, administrator powinien:
    1. Dokonać wpisu do prowadzonego rejestru naruszeń
    2. Wdrożyć środki zaradcze, tak by w przyszłości nie dochodziło do tego typu naruszeń
- **Prawdopodobne ryzyko** naruszenia praw lub wolności osób, których dane dotyczą, administrator powinien:
    1. Dokonać wpisu do prowadzonego rejestru naruszeń
    2. Wdrożyć środki zaradcze, tak by w przyszłości nie dochodziło do tego typu naruszeń
    3. Powiadomić organ nadzorczy o naruszeniu (PUODO)
    4. *Uzupełnić informację, gdyby pierwotne zawiadomienie (do 72h od zdarzenia) nie zawierało wszystkich informacji lub wystąpiły nowe istotne okoliczności*
- Występuje **wysokie ryzyko naruszenia praw lub wolności osób**, których dane dotyczą, administrator powinien:
    1. Dokonać wpisu do prowadzonego rejestru naruszeń
    2. Wdrożyć środki zaradcze, tak by w przyszłości nie dochodziło do tego typu naruszeń
    3. Powiadomić organ nadzorczy o naruszeniu (PUODO)
    4. Powiadomić osoby, których dane dotyczą o naruszeniu, jego potencjalnych skutkach oraz metodach zaradzenia im

5. *Uzupełnić informację, gdyby pierwotne zawiadomienie (do 72h od zdarzenia) nie zawierało wszystkich informacji lub wystąpiły nowe istotne okoliczności*
6. Kryteria oceny wagi naruszenia:

6.1. (DPC) Kontekst przetwarzania danych,

6.2. (EI) Łatwość identyfikacji osoby, które dane dotyczą,

6.3. (CB) Okoliczności naruszenia, mające dodatkowy wpływ na powagę (dotkliwość) naruszenia.

7. **Końcowy wynik oceny dotkliwości naruszenia (SE)**, po uwzględnieniu przyjętych wartości punktowych dla poszczególnych kryteriów można uzyskać korzystając z następującego wzoru:

SE = DPC x EI x CB

8. Przykład zastosowania algorytmu przyjętej procedury:

- **(DPC) Kontekst przetwarzania danych do 6.1.**
- Określenie rodzajów i klasyfikacja danych, których dotyczy naruszenie (przyjęto podział na:
  - Dane zwykłe,
  - Dane behawioralne,
  - Dane finansowe,
  - Dane szczególnych kategorii (wrażliwe)
- Ocena wystąpienia czynników dodatkowych, które mogły zwiększyć lub zmniejszyć wartość wskaźnika dla danego naruszenia
- **Łatwość identyfikacji osoby fizycznej (EI) do 6.2.**

Należy oszacować jak łatwo będzie podmiotowi, który ma nieuprawniony dostęp do danych, zidentyfikować osobę fizyczną, której dane dotyczą. W opisywanej metodologii określone zostały 4 poziomy tej kategorii:

- **Poziom niski (0,25)**
- **Poziom ograniczony (0,5)**
- **Poziom znaczny (0,75)**
- **Poziom wysoki (1)**

Przykład:

Naruszenie dotyczy Imienia i nazwiska klientów firmy

- *Poziom niski (0,25) – w całej populacji danego kraju bardzo wiele osób ma takie samo imię i nazwisko (Jan Kowalski)*
- *Poziom ograniczony (0,5) – w populacji kraju, niewiele osób ma takie same imię i nazwisko*
- *Poziom znaczny (0,75) – w danym regionie kilka osób ma takie samo imię i nazwisko*
- *Poziom wysoki (1) – w danym mieście jest tylko jedna osoba o takim imieniu i nazwisku*
- **Okoliczności naruszenia (CB) do 6.3.**

Dane naruszenie może dotyczyć:

- Utraty poufności danych:
  - 0 – gdy, dane mogły zostać narażone na utratę poufności, ale nie ma dowodów, że nastąpiło nielegalne przetwarzanie (np. laptop został zgubiony podczas transportu)
  - 0,25 – gdy dane mogły zostać ujawnione wielu znanym odbiorcom (np. wiadomość e-mail została błędnie przesłana do wielu znanych adresatów)
  - 0,5 – gdy dane zostały ujawnione wielu, nieznanym odbiorcom (np. opublikowanie danych na stronie Internetowej)

- Utraty integralności danych:
  - 0 – gdy dane zostały zmienione, ale nie zidentyfikowano nieprawidłowości (np. bazy z danymi osobowymi zostały błędnie zaktualizowane, ale administrator posiada wersje oryginalne – niezmienione)
  - 0,25 – gdy dane zostały zmienione i wykorzystane niepoprawnie, ale administrator może przywrócić poprawną wersję (np. zmieniono rekord niezbędny do świadczenia usługi online, a użytkownik musi poprosić o usługę offline)
  - 0,5 – gdy dane zostały zmienione i wykorzystane w niewłaściwy sposób, a administrator nie ma możliwości przywrócenia poprzedniej wersji

- Utraty dostępności danych:
  - 0 – gdy dane mogą zostać odzyskane bez trudności (np. utracono kopię pliku ale administrator dysponuje kopią zapasową)
  - 0,25 – gdy dane osobowe nie są dostępne przez jakiś czas (np. dane zostały utracone i konieczne jest ich ponowne zebranie)
  - 0,5 – gdy utracono dane osobowe i nie ma możliwości jej odtworzenia (np. nie istnieją kopie zapasowe ani nie można odtworzyć tych danych)

- Istotne jest także czy naruszenie było celowym czy przypadkowym działaniem:
  - 0,5 – gdy dane zostały utracone na skutek celowego działania (np. pracownik celowo przekazał dane klientów firmy jej konkurencji)

Ocena dotkliwości naruszenia bezpieczeństwa danych osobowych

Po analizie danego naruszenia, otrzymane wartości podstawiamy do wzoru:

SE = DPC x EI x CB

Otrzymany wynik oznacza:

SE < 2	Poziom Niski	Osoby fizyczne nie będą dotknięte tym naruszeniem lub mogą napotkać niewielkie niedogodności, które będą mogły bez problemu pokonać (np. ponownie należy poświęcić czas na wprowadzenie danych)
2 ≤ SE < 3	Poziom średni	Osoby fizyczne mogą napotkać znaczne trudności, które jednak będą w stanie pokonać (np. dodatkowe koszty, odmowa dostępu do usługi, stres)
3 ≤ SE< 4	Poziom wysoki	Osoby fizyczne będą dotknięte znacznymi konsekwencjami,

		które z pewnym trudem będą mogły pokonać (np. Umieszczenie na liście dłużników banku, uszkodzenie mienia, wezwanie do sadu, pogorszenie stanu zdrowia)
4 ≤ SE	Poziom bardzo wysoki	Osoby indywidualne mogą dotknąć znaczące a nawet nieodwracalne konsekwencje (np. kłopoty finansowe, niezdolność do pracy, dolegliwości psychiczne lub fizyczne, śmierć)

9. W przypadku, gdy procedurę przeprowadza IOD, Administrator ją akceptuje po zapoznaniu się z wynikiem i decyduje o czynnościach o których mowa w art. 33 i 34 RODO.

Zatwierdzam i nakazuję stosować.

Dyrektor
Szkoły Podstawowej Nr 2
im. Ks. Jana Twardowskiego
w Białymstoku
mgr Halina Puchalska

10.02.2025

data i podpis Administratora