PROCEDURA OCENY POWAGI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

W PRZEDSZKOLU MIEJSKIM NR 35 W BYTOMIU

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 (UODO) i/lub poinformowania osób fizycznych, których dane dotyczą na temat naruszenia, zgodnie z ciążącymi na administratorze obowiązkami określonymi w art. 33 i w art. 34 RODO. Dokument jest uzupełnieniem i doprecyzowaniem §13 przyjętej Polityki Bezpieczeństwa Ochrony Danych Osobowych w Przedszkolu Miejskim nr 35 w Bytomiu.

1. Procedura została opracowana na podstawie rekomendacji UODO. Odnosi się do wytycznych opublikowanych 30 maja 2019 r. pt. „Obowiązki administratorów związane z naruszeniami ochrony danych osobowych", 28 lutego 2019 r. pt. „Zasada przejrzystości a zawiadomienie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych" oraz „Rekomendacji dotyczących metodologii oceny powagi naruszenia danych osobowych przygotowanej przez Agencję Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA).
2. Przez naruszenie praw i wolności osób, których dane dotyczą rozumiemy powstanie uszczerbku fizycznego, szkód majątkowych lub niemajątkowych u osób fizycznych takich jak utrata kontroli nad własnymi danymi osobowymi lub ograniczenie praw, dyskryminacja, kradzież lub sfałszowanie tożsamości, strata finansowa, nieuprawnione odwrócenie pseudonimizacji, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową lub wszelkie inne znaczne szkody gospodarcze lub społeczne.
3. W przypadku naruszenia ochrony danych osobowych Administrator bez zbędnej zwłoki, w miarę możliwości nie później niż w terminie 24 godzin po stwierdzeniu naruszenia, zgłasza je Inspektorowi Ochrony Danych.
4. Za przeprowadzenie procedury oceny powagi naruszenia ochrony danych osobowych odpowiada Administrator. Ocenę poziomu naruszenia bezpieczeństwa danych osobowych konsultuje z Inspektorem Ochrony Danych.
5. Niezależnie od wyniku oceny (od niskiego, do bardzo wysokiego) incydent ten zostaje

odnotowany w prowadzonym przez administratora rejestrze incydentów/naruszeń.

6. Opis narzędzia oceny dotkliwości naruszenia/punktowej powagi naruszenia (miernika):
   6.1. Powaga naruszenia ochrony danych osobowych definiowana jest w kontekście metodologii jako „oszacowanie rozmiaru potencjalnego wpływu na osoby fizyczne spowodowanego przez naruszenie ochrony danych;

   6.2. Stosując tę metodologię, Administrator przechodzi przez cały proces wykorzystując określone kryteria ilościowe w celu przygotowania oceny;

   6.3. Ostateczną ocenę dotkliwości powagi naruszenia można uzyskać stosując następujący wzór: SE = DPC x EI + CB;

   6.4. Kontekst przetwarzania danych (DPC) Dotyczy typu danych będących przedmiotem naruszenia wraz z czynnikami powiązanymi z ogólnym kontekstem przetwarzania. DPC jest najważniejszym elementem metodologii i służy do oceny krytyczności określonego zbioru danych w określonym kontekście przetwarzania;

   6.5. Łatwość identyfikacji (EI) Określa poziom łatwości zidentyfikowania osoby, której dane dotyczą. Poziom niski występuje w sytuacji, gdy łatwość identyfikacji jest niewielka, co oznacza, że połączenie danych z określoną osobą jest bardzo trudne, ale w pewnych warunkach możliwe. Poziom maksymalny oznacza, że identyfikacja jest możliwa bezpośrednio przy pomocy danych będących przedmiotem naruszenia bez konieczności prowadzenia innych działań, aby określić tożsamość danej osoby.

   6.6. Okoliczności naruszenia (CB) Dotyczą konkretnych okoliczności naruszenia powiązanych z typem naruszenia, w tym głównie utraty bezpieczeństwa danych będących przedmiotem naruszenia oraz jakiegokolwiek powiązanego z naruszeniem umyślnego działania. CB określa konkretne okoliczności naruszenia, które mogą wystąpić lub nie w określonej sytuacji. Dlatego też, jeżeli występuje, CB może tylko zwiększyć powagę naruszenia ochrony danych. Z tego powodu wstępna ocena punktowa może zostać dalej dostosowana za pomocą CB;

   6.7. Wynik ten znajduje się w określonym przedziale wartości, który odpowiada jednemu z czterech poziomów powagi naruszenia: niskie, średnie, wysokie i bardzo wysokie;

   6.8. Po określeniu poziomu powagi naruszenia, może on zostać opatrzony również oznaczeniem, wskazującym określone elementy naruszenia, które nie wpływają na

wynik, ale mają znaczenie dla ostatecznej oceny. Dla potrzeb niniejszej metodologii określono dwa rodzaje oznaczeń:

6.8.1. Liczba podmiotów danych, których dotyczy naruszenie przekracza 100. Ujawnienie danych podmiotu danych naruszonych w ramach większego zdarzenia może być łatwiejsze, natomiast jednocześnie większa liczba podmiotów danych wpływa na ogólna skalę naruszenia,

6.8.2. Nieczytelne dane. Nieczytelność (np. mocne zaszyfrowanie bez ujawnienia klucza) może znacząco zmniejszyć wpływ na podmioty danych, ponieważ znacząco zmniejsza możliwość, że osoby nieupoważnione uzyskają dostęp do danych.

7. Ocena dotkliwości naruszenia

7.1. (DPC) Kontekst przetwarzania danych.

Określenie rodzajów i klasyfikacja danych, których dotyczy naruszenie:

- Dane zwykłe (1-4) – ocena wyjściowa 1,
- Dane behawioralne (1-4) – ocena wyjściowa 2,
- Dane finansowe (1-4) – ocena wyjściowa 3,
- Dane szczególnych kategorii (wrażliwe) (1-4) – ocena wyjściowa 4.

Oceny punktowej kontekstu przetwarzania danych Administrator dokonuje zgodnie z załącznikiem nr 1. Dokonując oceny Administrator powinien zwrócić szczególną uwagę na numer PESEL. Zgodnie z opinią Prezesa Urzędu Ochrony Danych Osobowych (PUODO) naruszenie obejmujące utratę poufności w stosunku do numeru PESEL wraz z innymi danymi umożliwiającymi identyfikację np. imię i nazwisko wiąże się z dużym ryzykiem naruszenia praw lub wolności osób, których dane dotyczą. W związku z tym, że metodologia nie uwzględnia tego czynnika ze względu na swoje międzynarodowe zastosowanie. Uzupełniono kontekst przetwarzania w załączniku nr 1.

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

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).

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

Należy oszacować okoliczności naruszenia, mające dodatkowy wpływ na powagę tj.;

• Utraty poufności danych (NP) - informacje uzyskują strony, które nie są upoważnione do takiego dostępu. Zakres utraty poufności różni się w zależności od zasięgu ujawnienia, tzn. ewentualnej liczby i rodzaju stron, które mogą mieć bezprawny dostęp do informacji:

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).

Informacje uzyskują strony, które nie są upoważnione do takiego dostępu. Zakres utraty poufności różni się w zależności od zasięgu ujawnienia, tzn. ewentualnej liczby i rodzaju stron, które mogą mieć bezprawny dostęp do informacji

• Utraty integralności danych (NI) - oryginalne informacje zostają zmodyfikowane, a taka zmiana danych może być niekorzystna dla podmiotu 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 (ND) - nie ma dostępu do oryginalnych danych w sytuacji, gdy jest to potrzebne:

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 (IDS):
+0,5 – gdy dane zostały utracone na skutek celowego działania (np. pracownik celowo przekazał dane klientów firmy jej konkurencji).

7.4. Końcowy wynik oceny okoliczności naruszenia (CB), po uwzględnieniu przyjętych wartości punktowych dla poszczególnych kryteriów można uzyskać korzystając z następującego wzoru:

CB=NP+NI+ND+IDS

7.5. W przypadku incydentu odnoszącego się do kliku rodzajów danych osobowych, Administrator wykonuje ocenę powagi naruszenia ochrony danych, dla każdego osobno. Do podjęcia decyzji o zakwalifikowaniu naruszenia wymagającego lub nie, zgłoszenia do UODO i/lub poinformowania osób fizycznych, których dane dotyczą przyjmuję się najwyższy wynik oceny dotkliwości naruszenia.

7.6. 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),

• $2 \leq SE < 3$

Poziom średni

Osoby fizyczne mogą napotkać znaczne trudności, które jednak będą w stanie pokonać

(np. dodatkowe koszty, odmowa dostępu do usługi, stres),

- $3 \leq SE < 4$

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),

- $4 \leq SE$

Poziom bardzo wysoki

Osoby indywidualne mogą dotknąć znaczące a nawet nieodwracalne konsekwencje (np. kłopoty finansowe, niezdolność do pracy, dolegliwości psychiczne lub fizyczne, śmierć).

8. Jeżeli dane naruszenie powoduje:

8.1. ($SE < 2$) - 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.

8.2. ($2 \leq SE < 3$) - 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. Potencjalnie powiadomić organ nadzorczy o naruszeniu (UODO);

4. Uzupełnić informację, gdyby pierwotne zawiadomienie (do 72h od zdarzenia) nie zawierało wszystkich informacji lub wystąpiły nowe istotne okoliczności;

5. W przypadku wskazania przez organ nadzorczy, Powiadomić osoby, których dane dotyczą o naruszeniu, jego potencjalnych skutkach oraz metodach zaradzenia im.

8.3. ($3 \leq SE < 4$) - 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 (UODO);

4. Potencjalne 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. W przypadku wskazania przez organ nadzorczy, Powiadomić osoby, których dane dotyczą o naruszeniu, jego potencjalnych skutkach oraz metodach zaradzenia im

8.4. (4 ≤ SE) - Występuje bardzo 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 (UODO);

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. Po zakończeniu oceny, Administrator bierze pod uwagę inne ewentualnie pasujące kryteria (liczba osób oraz nieczytelność danych), które nie zostały uwzględnione w metodologii, ale powinny być oceniane i oznaczane, które mają znaczenie dla ostatecznej oceny (małe prawdopodobieństwo dostępu do danych osobowych występuję w przypadku szyfrowania danych lub pseudonimizacji. Wówczas, gdy poziom zabezpieczenia uniemożliwia nieuprawniony dostęp do danych).

7. Decyzję o zakwalifikowaniu naruszenia wymagającego lub nie, zgłoszenia do UODO i/lub poinformowania osób fizycznych, których dane dotyczą na temat

zdarzenia podejmuję ostatecznie Administrator po przeprowadzeniu oceny zgodnie z procedurą i uwzględniając całościowy kontekst zdarzenia.

8. Zgłoszenia do UODO dokonuję Administrator zgodnie z art. 33 RODO i §13 przyjętej Polityki Bezpieczeństwa Ochrony Danych Osobowych w Przedszkolu Miejskim nr 35 w Bytomiu i obowiązującymi wytycznymi UODO.

9. Zawiadomienia osób, której dane dotyczą na temat naruszenia dokonuje Administrator zgodnie z art. 34 RODO za pośrednictwem dostępnych środków komunikacji tak, aby dochować niezwłoczności powiadomienia. Dobierając kanał komunikacji z podmiotem danych, należy cały czas pamiętać o możliwości wykazania, że zawiadomienie zostało przez administratora przekazane.

10. Zawiadomienie, o którym mowa powyżej, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz co najmniej:

- opisuje charakter naruszenia ochrony danych osobowych,
- opisuje możliwe konsekwencje naruszenia ochrony danych osobowych,
- opisuje 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 (zalecenia dla osoby fizycznej, co do minimalizacji potencjalnych niekorzystnych skutków),
- zawiera imię i nazwisko oraz dane kontaktowe IOD lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji.

11. Obowiązek powiadomienia jest wyłączony w przypadku, gdy (art. 34 ust. 3 RODO):

- Administrator wdrożył odpowiednie środki bezpieczeństwa i uniemożliwił dostęp do danych objętych naruszeniem osobom nieupoważnionym,
- Administrator zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia,
- powiadomienie wymagałoby niewspółmiernie dużego wysiłku i administrator wydał publiczny komunikat o naruszeniu lub zastosował inne podobne rozwiązanie.

12. Procedura obowiązuje od dnia: 31 sierpnia 2021r.