ZARZĄDZENIE NR 83/2023
Dyrektora Miejskiego Ośrodka Pomocy Rodzinie
w Piekarach Śląskich
z dnia 27.12.2023r.

w sprawie: powołania komisji do spraw oceny naruszeń bezpieczeństwa danych osobowych.

Na podstawie § 10 ust. 1 pkt 7 Regulaminu Organizacyjnego Miejskiego Ośrodka Pomocy Rodzinie w Piekarach Śląskich wprowadzonego Zarządzeniem nr 56/MOPR/2023 Prezydenta Miasta Piekary Śląskie z dnia 20 stycznia 2023 roku oraz mając na uwadze treść przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016r. w sprawie ochrony osób fizycznych oraz Ustawy z dnia 10 maja 2018r. o ochronie danych osobowych (t.j. Dz. U. z 2019r., poz. 1781)

zarządzam, co następuje:

§ 1

Powołanie komisji do spraw oceny naruszeń i incydentów związanych z bezpieczeństwem danych osobowych w następującym składzie:

1. Maciej Gazda – przewodniczący
2. Mirosława Kusz - członek
3. Dawid Kawałek – członek.

§ 2

Wprowadza się do stosowania w Miejskim Ośrodku Pomocy Rodzinie w Piekarach Śląskich:

1) Protokół Komisji dokonującej naruszenia związanego z bezpieczeństwem danych osobowych stanowiący Załącznik nr 1 do Niniejszego Zarządzenia;
2) Procedurę Oceny Wagi Naruszenia Ochrony Danych Osobowych stanowiącą Załącznik nr 2 do niniejszego Zarządzenia.

§ 3

Wykonanie Zarządzenia powierzam:
- Administratorowi Danych Osobowych,
- Inspektorowi Ochrony Danych,
- Kierownikowi Działu Organizacji, Kadr i Płac.

§ 4

Zarządzenie wchodzi w życie z dniem podjęcia.

Maciej Gazda
Dyrektor
Miejskiego Ośrodka Pomocy Rodzinie
w Piekarach Śląskich

Załącznik nr 1
do Zarządzenia nr 83/2023
Dyrektora Miejskiego Ośrodka Pomocy Rodzinie
w Piekarach Śląskich
z dnia 27.12.2023r.
w sprawie powołania komisji ds. oceny naruszeń
i incydentów związanych z bezpieczeństwem danych
osobowych

Protokół komisji

W dniu ……..…….Komisja w składzie:

1. Maciej Gazda – przewodniczący
2. Mirosława Kusz - członek
3. Dawid Kawałek - członek

dokonała oceny naruszenia związanego z bezpieczeństwem danych osobowych :
……..
……..……...
……

Podpisy:

1) ……
2) ……
3) ……...

Załącznik nr 2
do Zarządzenia nr 83/2023
Dyrektora Miejskiego Ośrodka Pomocy Rodzinie
w Piekarach Śląskich
z dnia 27.12.2023r.
w sprawie powołania komisji ds. oceny naruszeń
i incydentów związanych z bezpieczeństwem danych
osobowych

PROCEDURA OCENY WAGI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Celem procedury jest ocena poziomu naruszenia bezpieczeństwa danych osobowych (ich dostępności, poufności, integralności oraz rozliczalności) w celu zakwalifikowania zdarzenia wymagającego lub nie wymagającego 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 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 naruszenia ochrony danych osobowych odpowiada wyznaczona komisja.

4. Niezależnie od wyniku oceny (od niskiego do bardzo wysokiego), incydent ten zostaje odnotowany w prowadzonym przez inspektora ochrony danych rejestrze incydentów.

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

6. Według metody **ENISA**, do określenia wagi naruszenia są potrzebna następujące informacje:
   a) kontekst przetwarzania danych **KPD,**
   b) prawdopodobieństwo identyfikacji **PI**,
   c) okoliczności naruszenia **ON**,
   z których wyliczamy, że **Waga naruszenia = KPD * PI + ON**

7. **Kontekst przetwarzania danych.**
   Pierwszy czynnik brany pod uwagę to KPD. Składa się on z dwóch składników: rodzaju danych oraz kontekstu podwyższającego lub obniżającego. Najpierw należy ustalić rodzaj danych. Metoda proponuje następujące rodzaje, z matematyczną punktacją:
   - dane podstawowe (1 punkt),
   - dane dotyczące zachowań osoby (2 punkty),

- dane finansowe (3 punkty),
- dane szczególnych kategorii (4 punkty).

Ocenę kontekstu może podwyższyć lub obniżyć każdy z poniższych elementów:

- szeroki zakres danych tej samej osoby (+1) – szeroki zarówno w znaczeniu liczby kategorii danych, jak i czasu przez jaki podlegały naruszeniu;
- możliwe negatywne skutki dla podmiotu danych (+1);
- charakter danych (+1/-1) – przykładowo zaświadczenie lekarskie o idealnym stanie zdrowia będzie obniżało wycenę, pomimo że to dane szczególnej kategorii, a zaświadczenie o wstydliwej chorobie dodatkowo podwyższało;
- specyfika podmiotu danych (+1/-1) – inaczej wycenimy dane celebrytów, inaczej dzieci, a inaczej pracowników służb bezpieczeństwa;
- specyfika administratora (+1/-1)
- publiczna dostępność danych przed naruszeniem (-1);
- nieaktualność danych (-1)

8. **Prawdopodobieństwo identyfikacji.**

Skala prawdopodobieństwa obejmuje cztery stopnie:

a) znikome (0,25),
b) ograniczone (0,5),
c) wysokie (0,75),
d) maksymalne (1).

9. **Okoliczności naruszenia**

Ostatni element głównego wzoru podwyższa wagę naruszenia z uwagi na kilka aspektów:

- +0,25 pkt – nastąpiło naruszenie poufności, a dane zostały ujawnione znanym odbiorcom, więc można się do nich zwrócić i podjąć działania minimalizujące szkodę;
- +0,5 pkt – nastąpiło naruszenie poufności, a dane ujawniono nieznanym odbiorcom;
- +0,25 pkt – nastąpiło naruszenie integralności, lecz dane da się naprawić;
- +0,5 pkt – nastąpiło naruszenie integralności, a naprawa danych jest niemożliwa;
- +0,25 pkt – nastąpiło naruszenie dostępności, lecz dane można odzyskać;
- +0,5 pkt – nastąpiło naruszenie dostępności, a danych nie da się odzyskać;
- +0,5 pkt – naruszenie nastąpiło w wyniku zamierzonego, intencjonalnego działania sprawcy, a nie w wypadku omyłki lub zdarzenia losowego.

10. **Ostateczne określenie wagi naruszenia**

Gdy wszystkie elementy ostatecznego wzoru zostaną poprawnie oszacowane, ostateczny wynik **(waga = KPD * PI + ON)** pozwoli na rozpoznanie, z którym z przypadków mamy do czynienia:

1) osoby nie zostaną dotknięte naruszeniem lub wywoła ono drobne niedogodności (waga < 2),
2) osoby mogą napotkać niedogodności, które są możliwe do pokonania (waga < 3),
3) mogą wystąpić konsekwencje możliwe do pokonania, ale z poważnymi skutkami (waga < 4),
4) mogą wystąpić znaczące, nawet nieodwracalne konsekwencje (dla wag od 4 w górę).

.