Zarządzenie nr 51/2023
Dyrektora Miejskiego Ośrodka Sportu i Rekreacji w Sosnowcu
z dnia 28 czerwca 2023 roku

w sprawie zmiany Zarządzenia nr 50/2018 Dyrektora Miejskiego Ośrodka Sportu i Rekreacji w Sosnowcu z dnia 25 maja 2018 roku w sprawie zatwierdzenia Polityki bezpieczeństwa przetwarzania danych osobowych w Miejskim Ośrodku Sportu i Rekreacji w Sosnowcu

Na podstawie § 8 ust. 3 Statutu Miejskiego Ośrodka Sportu i Rekreacji w Sosnowcu oraz § 6 ust. 2 pkt c Regulaminu organizacyjnego Miejskiego Ośrodka Sportu i Rekreacji w Sosnowcu w związku z art. 24 ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),

zarządzam co następuje:

§ 1

1.Zmienić treść Rozdziału 5 Załącznika do Zarządzenia nr 50/2018 Dyrektora Miejskiego Ośrodka Sportu i Rekreacji w Sosnowcu z dnia 25 maja 2018 roku w sprawie zatwierdzenia Polityki bezpieczeństwa przetwarzania danych osobowych w Miejskim Ośrodku Sportu i Rekreacji w Sosnowcu i nadać mu brzemiennie ustalone w Załączniku nr 1 do niniejszego Zarządzenia.
2. Dodać do Załącznika do Zarządzenia nr 50/2018 Dyrektora Miejskiego Ośrodka Sportu i Rekreacji w Sosnowcu z dnia 25 maja 2018 roku w sprawie zatwierdzenia Polityki bezpieczeństwa przetwarzania danych osobowych w Miejskim Ośrodku Sportu i Rekreacji w Sosnowcu
Załącznik Nr 16 „Procedura postępowania z incydentami i naruszeniami ochrony danych osobowych".

§ 2

Pozostałe postanowienia Zarządzenia pozostają bez zmian.

§ 3

Wykonanie zarządzenia powierzam Inspektorowi Ochrony Danych, Zastępcom Dyrektora, Głównemu Księgowemu, kierownikom komórek organizacyjnych i pracownikom zatrudnionym na samodzielnych stanowiskach oraz pracownikom i współpracownikom przetwarzającym dane osobowe w Miejskim Ośrodku Sportu i Rekreacji w Sosnowcu.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
Jerzy Górak

Załącznik Nr 1
do Zarządzenia Nr 51/2023
Dyrektora Miejskiego Ośrodka
Sportu i Rekreacji w Sosnowcu
z dnia 27 czerwca 2023 roku

Rozdział 5

Postępowanie w przypadku incydentów bezpieczeństwa danych osobowych

1. Wszyscy pracownicy i współpracownicy MOSiR zobowiązani są do natychmiastowego zgłaszania ADO i/lub IOD lub bezpośredniemu przełożonemu incydentów związanych z naruszeniem bezpieczeństwa przetwarzania danych osobowych.

2. IOD, w ciągu 72 godzin od momentu zgłoszenia naruszenia, dokonuje jego oceny, zasadności oraz ustalenia stanu faktycznego przy wsparciu Pomocy informatycznej oraz innych osób, których wiedza lub wyjaśnienia mogą być pomocne.

3. W przypadku ustalenia powyższych informacji, IOD przekazuje rekomendację do ADO.

4. ADO, bez zbędnej zwłoki, jednakże nie później niż w ciągu 72 godzin od momentu wykrycia naruszenia, zgłasza to naruszenie, wraz z ustaleniami IOD, organowi nadzorczemu PUODO. Zgłoszenie odbywa się zgodnie z wymogami art. 33 RODO.

5. Nie jest wymagane dokonanie zgłoszenia, o którym mowa w ust. 3, o ile jest mało prawdopodobne, by dane naruszenie skutkowało ryzykiem naruszenia praw i wolności osób fizycznych.

6. IOD zobowiązany jest prowadzić rejestr incydentów związanych z naruszeniem bezpieczeństwa przetwarzania danych osobowych, zgodnie z Załącznikiem Nr 12.

DYREKTOR
Jerzy Górak

Załącznik Nr 2

do Zarządzenia Nr 51/2023 Dyrektora
Miejskiego Ośrodka Sportu i Rekreacji w Sosnowcu
z dnia 28 czerwca 2023 roku

Załącznik Nr 16

do „Polityki bezpieczeństwa przetwarzania danych osobowych w Miejskim Ośrodku Sportu i Rekreacji w Sosnowcu"

Procedura postępowania z incydentami i naruszeniami ochrony danych osobowych

Rozdział 1

CEL

Celem procedury jest:

1) minimalizacja skutków wystąpienia incydentów i naruszeń bezpieczeństwa;

2) ograniczenie ryzyka występowania incydentów i naruszeń w przyszłości;

3) prawidłowe reagowanie osób upoważnionych do przetwarzania danych osobowych oraz osób upoważnionych do przebywania w obszarze przetwarzania danych osobowych w przypadku stwierdzenia incydentu lub naruszenia ochrony danych osobowych;

4) zgłaszanie naruszeń ochrony danych osobowych organowi nadzorczemu oraz osobom, których dane dotyczą.

Rozdział 2

ZAKRES STOSOWANIA

Procedurę stosuje się do wszystkich osób upoważnionych do przetwarzania danych osobowych, zarówno zatrudnionych jak i wykonujących czynności na podstawie odrębnych umów.

Rozdział 3

TRYB POSTĘPOWANIA

1. Procedura definiuje katalog incydentów i naruszeń zagrażających bezpieczeństwu danych osobowych, jednakże nie jest on zamknięty, oraz opisuje sposób reagowania na nie.

2. Incydent to możliwość wystąpienia ujawnienia, utraty lub niedostępności danych. Jest to sytuacja, która może prowadzić do naruszenia, czyli potwierdzonego już ujawnienia, utraty lub niedostępności danych.

3. Odpowiedzialność za prawidłowe zgłaszanie incydentów dotyczących bezpieczeństwa danych osobowych spoczywa na osobach upoważnionych oraz osobach upoważnionych do przebywania w obszarze przetwarzania danych osobowych dokonujących zgłoszeń.

4. Wszyscy pracownicy, przełożeni, ASI oraz IOD współpracują ze sobą po zgłoszeniu incydentu lub naruszenia bezpieczeństwa i odpowiedzialni są za:

4.1. niezwłoczne reagowanie na incydenty lub naruszenia bezpieczeństwa danych osobowych w określony i z góry ustalony sposób;

4.2. ocenę istniejących i potencjalnych incydentów lub naruszeń w zakresie bezpieczeństwa danych osobowych;

4.3. ocenę przyczyn i skutków incydentów oraz naruszeń bezpieczeństwa danych osobowych w tym gromadzenie materiału dowodowego;

4.4. przygotowywanie propozycji działań korygujących i naprawczych oraz nadzór nad ich wprowadzaniem.

5. ADO odpowiedzialny jest za:

5.1. ocenę wymagalności zgłoszenia naruszenia bezpieczeństwa danych osobowych do organu nadzorczego PUODO oraz osób, których dane dotyczą, po konsultacji z IOD i/lub ASI (jeśli naruszenie dotyczy systemu informatycznego);

5.2. przygotowanie treści zgłoszenia dotyczącego naruszenia bezpieczeństwa danych osobowych do organu nadzorczego PUODO oraz osób, których dane dotyczą we współpracy z IOD;

5.3. nadzór nad wprowadzaniem działań korygujących i naprawczych.

6. Do typowych incydentów bezpieczeństwa danych osobowych należą:

6.1. naruszenie lub wadliwe funkcjonowanie zabezpieczeń fizycznych w pomieszczeniach (np. wyłamane lub zacinające się zamki, naruszone plomby, niedomykające się bądź wybite okna, itp.) nie powodujące utraty, ujawnienia, niedostępności danych;

6.2. utrata usługi, urządzenia lub funkcjonalności nie powodująca utraty, ujawnienia, niedostępności danych;

6.3. nieautoryzowana modyfikacja nie powodująca utraty, ujawnienia, niedostępności danych;

6.4. pożar, zalanie nie powodujące utraty, ujawnienia, niedostępności danych;

6.5. pozyskiwanie oprogramowania z nielegalnych źródeł;

6.6. pojawianie się nietypowych komunikatów na ekranie;

6.7. niemożność zalogowania się do systemu teleinformatycznego;

6.8. spowolnienie pracy oprogramowania;

6.9. niestabilna praca systemu teleinformatycznego;

6.10. brak reakcji systemu na działania użytkownika;

6.11. ponowny start lub zawieszanie się komputera;

6.12. ograniczenie funkcjonalności oprogramowania.

7. Za naruszenie zasad ochrony danych osobowych uważa się w szczególności:

7.1. nieupoważniony dostęp, modyfikacje, kopiowanie, udostępnienie lub zniszczenie/usunięcie danych osobowych, zarówno w systemie teleinformatycznym, jak i na nośnikach papierowych i elektronicznych;

7.2. udostępnianie danych osobowych nieuprawnionym podmiotom;

7.3. nieautoryzowany dostęp do danych osobowych przez połączenie sieciowe;

7.4. niedopełnienie obowiązku ochrony danych osobowych przez umożliwienie dostępu do danych osobowych (np. pozostawienie kopii danych osobowych, nie zablokowanie dostępu do systemu, pozostawienie dokumentów z danymi osobowymi w miejscu dostępnym dla osób nieuprawnionych, brak nadzoru nad serwisantami i innymi osobami nieuprawnionymi przebywającymi w pomieszczeniach, gdzie przetwarza się dane osobowe);

7.5. stworzenie niezabezpieczonego kanału dystrybucji danych osobowych;

7.6. nielegalne bądź nieświadome ujawnienie danych osobowych;

7.7. niepodjęcie działań zmierzających do eliminacji wirusów komputerowych lub innych programów zagrażających integralności systemu teleinformatycznego;

7.8. ujawnienie indywidualnych haseł dostępu do danych osobowych w systemie;

7.9 przesyłanie danych osobowych przez Internet bez zabezpieczenia;

7.10. przesyłanie dokumentów papierowych i nośników elektronicznych z danymi osobowymi bez zabezpieczenia osobom nieuprawnionym;

7.11. wykonanie nieuprawnionych kopii danych osobowych;

7.12. kradzież nośników zawierających dane osobowe lub oprogramowanie;

7.13. kradzież sprzętu służącego do przetwarzania danych osobowych;

7.14. spowodowanie utraty danych osobowych w systemie teleinformatycznym, na kopiach bezpieczeństwa i na innych nośnikach;

7.15. dopuszczenie do braku aktualnych kopii bezpieczeństwa danych osobowych lub brak odpowiednich nośników do sporządzania kopii;

7.16. niewłaściwe niszczenie nośników z danymi osobowymi pozwalające na ich odczyt;

7.17. naruszenie zasad ochrony fizycznej pomieszczeń, w których przetwarza się dane osobowe;
7.18. dopuszczenie do przetwarzania danych osobowych pracowników bez odpowiednich upoważnień;

7.19. brak szkoleń pracowników w zakresie zasad bezpieczeństwa danych osobowych;

7.20. pożar, zalanie powodujące utratę, ujawnienie lub niedostępność danych;

7.21. inne sytuacje wskazujące lub potwierdzające naruszenie bezpieczeństwa danych osobowych.

8. Osoby upoważnione, osoby upoważnione do przebywania w obszarze przetwarzania danych osobowych oraz podmioty przetwarzające mają obowiązek zgłaszania wszystkich incydentów i naruszeń dotyczących ochrony danych osobowych.

9. Osoba upoważniona, i wymienione w pkt. 8, poprzez przełożonego zgłasza incydent i naruszenia dotyczące ochronnych danych osobowych do IOD i/lub ASI. W sytuacji braku możliwości dokonania zgłoszenia poprzez przełożonego, osoba zgłaszająca kontaktuje się bezpośrednio z IOD i/lub ASI.

9.1. Osoba upoważniona zgłasza incydenty i naruszenia za pośrednictwem formularza zgłoszenia incydentu (załącznik Nr 11, uzupełnia treść w części dla osoby zgłaszającą zdarzenie), poczty elektronicznej lub w przypadku konieczności natychmiastowej reakcji – telefonicznie lub osobiście. Po zgłoszeniu ustnym lub telefonicznym osoba zgłaszająca zobowiązana jest wysłać uzupełniające zgłoszenia lub złożyć zgłoszenie w formie papierowej w najbliższym możliwym terminie. IOD może zamiast osoby zgłaszającej uzupełnić treść zgłoszenia na podstawie pisemnej informacji przekazanej IOD przez osobę zgłaszającą incydent, naruszenie. IOD dołącza tę informację do formularza zgłoszenia incydentu.

9.2. Formularz zgłoszenia incydentu rejestrowany jest w prowadzonej przez IOD ewidencji incydentów naruszenia bezpieczeństwa zgodnie z Załącznikiem Nr 12.

10. Na stanowisku, na którym stwierdzono naruszenie bezpieczeństwa danych osobowych przełożony, ASI lub IOD przejmują nadzór nad pracą na zagrożonym stanowisku pracy, odsuwając jednocześnie od stanowiska osobę, która dotychczas na nim pracowała, aż do czasu wydania odmiennej decyzji.

11. Wszelkie działania związane z samodzielnym naprawianiem, potwierdzaniem lub testowaniem potencjalnych słabości systemu są zabronione.

12. Dokonywanie zmian w miejscu incydentu lub naruszenia ochrony danych osobowych bez wiedzy i zgody przełożonego, ASI lub Inspektora Ochrony Danych (w zależności od rodzaju naruszenia), jest dopuszczalne jedynie w sytuacji, gdy zachodzi konieczność ratowania życia lub zdrowia osób oraz mienia w przypadku ich bezpośredniego zagrożenia.

13. Przełożony, ASI oraz IOD przy wspólnej współpracy podejmują działania niezwłocznie po zgłoszeniu incydentu lub naruszenia.

13.1.Zobowiązani są oni do przeprowadzenia postępowania wyjaśniającego w toku, którego:

a) ustalają zakres i przyczyny zagrożenia oraz jego ewentualne skutki;

b) inicjują ewentualne działania dyscyplinarne;

c) rekomendują działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości.

14. W toku prowadzonego postępowania wyjaśniającego można udokumentować okoliczności naruszenia poprzez:

a) sporządzenie notatki z przeprowadzonych oględzin miejsca zdarzenia;

b) sporządzenie kopii obrazu wyświetlonego na ekranie monitora komputera związanego z naruszeniem;

c) sporządzenie kopii zapisów rejestrów systemu informatycznego służącego do przetwarzania danych osobowych lub zapisów konfiguracji technicznych środków zabezpieczeń sytemu;

d) odebranie pisemnych wyjaśnień od osoby, która ujawniła naruszenie.

15. Na podstawie dokonanych ustaleń, IOD wypełnia treść formularza zgłoszenia incydentu (Załącznik Nr 11) w zakresie opisu charakteru naruszenia, określa kategorię i przybliżoną liczbę osób, których dane dotyczą i możliwe konsekwencje naruszenia ochrony danych oraz w zakresie wskazania środków zastosowanych w celu zarządzania minimalizacją negatywnych skutków naruszenia ochrony danych, informacji o terminie powiadomienia organu nadzorczego PUODO wraz z uzasadnieniem oraz w zakresie informacji czy i kiedy zostały powiadomione osoby, których dane dotyczą wraz z uzasadnieniem.

16. Na podstawie przeprowadzonego postępowania wyjaśniającego oraz zebranych dowodów i po konsultacji z IOD, ADO dokonuje oceny istotności incydentu oraz wymagalności zgłoszenia naruszenia ochrony danych osobowych do organu nadzorczego.

17. W przypadku istotnych incydentów, a przede wszystkim incydentów, które mogą powodować ryzyko naruszenia praw i wolności osób, których dane dotyczą, ADO w porozumieniu z IOD tworzy plan działań mających na celu ograniczenie możliwości powstania incydentów podobnego typu w przyszłości.

18. IOD dokonuje przeglądu Rejestru incydentów regularnie przynajmniej raz na kwartał.

18.1. Przegląd obejmuje określenie: liczby incydentów bądź naruszeń, incydentów powtarzających się, trendów(te same błędy) związanych z incydentami bezpieczeństwa, kosztów (straty oraz nakłady finansowe) związanych z incydentami bezpieczeństwa, formułowanie wniosków z przeprowadzonego przeglądu.
18.2. Powyższe informacje zostają opisane w raporcie z przeglądu incydentów, który stanowi dane przekazywane ADO. ADO, w porozumieniu z IOD, na podstawie m.in. tych danych, określa dobór środków jakie muszą być wdrożone, aby do dalszych takich naruszeń nie dochodziło.

19. W przypadku stwierdzenia działań umyślnych i ustaleniu sprawcy incydentu, IOD przekazuje wyniki analizy wraz z zabezpieczonym materiałem dowodowym ADO celem ewentualnego zawiadomienia organów ścigania lub podjęcia kroków prawnych wobec osób trzecich.

20. Przy ocenie wymagalności zgłoszenia naruszenia ochrony danych osobowych do organu nadzorczego, ADO wraz z IOD biorą pod uwagę następujące skutki przetwarzania danych, które mogą powodować ryzyko naruszenia praw i wolności osób, których dane dotyczą:

a) kradzież tożsamości;

b) straty finansowe;

c) naruszenie dobrego imienia;

d) naruszenie poufności danych chronionych tajemnicą zawodową;

e) utrata przysługujących osobom praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi;

f) ujawnienie szczególnych kategorii danych.

21. Naruszenia ochrony danych osobowych podlegają zgłoszeniu organowi nadzorczemu.

22. Zgłoszeń naruszeń do organu nadzorczego dokonuje ADO bez zbędnej zwłoki, lecz nie później niż w terminie 72 godzin po stwierdzeniu naruszenia.

23. W przypadku braku zgłoszenia naruszenia w terminie do 72 godzin, ADO zobowiązany jest dołączyć do zgłoszenia wyjaśnienia dotyczące przyczyny opóźnienia.

24. Zgłoszenie do organu nadzorczego obejmuje:

a) opis charakteru naruszenia ochrony danych osobowych, w tym wskazanie kategorii i przybliżonej liczby osób, których dane dotyczą oraz kategorię i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;

b) imię i nazwisko oraz dane kontaktowe IOD, od którego można uzyskać więcej informacji;

c) opis możliwych konsekwencji naruszenia ochrony danych osobowych;

d) opis środków zastosowanych lub proponowanych przez ADO w celu zaradzenia naruszenia ochrony danych osobowych.

25. W przypadku, jeżeli nie da się udzielić informacji wymaganych w zgłoszeniu w tym samym czasie, należy je udzielać sukcesywnie bez zbędnej zwłoki.

26. ADO nie będzie zobligowany do powiadomienia organu nadzorczego, jeżeli wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zastosował do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych.

27. Jeżeli naruszenie bezpieczeństwa danych osobowych będzie mogło powodować wysokie ryzyko naruszenia praw i wolności osób, ADO zobligowany jest poinformować o naruszeniu danych osoby, których dane dotyczą.

28. Powiadomienie o naruszeniu należy dokonać bez zbędnej zwłoki, jasnym, prostym językiem.

29. ADO nie będzie zobligowany do powiadomienia osób, których dane dotyczą, jeżeli wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zastosował do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych.

DYREKTOR
Jerzy Górak