Zarządzenie Nr 14/2021

Dyrektora Miejskiego Ośrodka Pomocy Społecznej w Wąbrzeźnie
z dnia 18 października 2021 roku

w sprawie wprowadzenia Procedury postępowania w przypadku naruszenia ochrony danych osobowych w Miejskim Ośrodku Pomocy Społecznej w Wąbrzeźnie

Na podstawie: art. 33 i 34 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. 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

Wprowadza się do stosowania „Procedurę postępowania w przypadku naruszenia ochrony danych osobowych w Miejskim Ośrodku Pomocy Społecznej w Wąbrzeźnie" w brzmieniu stanowiącym załącznik do niniejszego zarządzenia.

§ 2

Zobowiązuje się wszystkich pracowników jednostki upoważnionych do przetwarzania danych osobowych do zapoznania się z niniejszym zarządzeniem.

§ 3

Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik nr 1 do Zarządzenia Nr 14/2021 Dyrektora Miejskiego Ośrodka Pomocy Społecznej w Wąbrzeźnie z dnia 18 października 2021 r.

PROCEDURA POSTĘPOWANIA W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH W MIEJSKIM OŚRODKU POMOCY SPOŁECZNEJ W WĄBRZEŹNIE

§ 1.

Ilekroć w niniejszej procedurze użyto określeń:

1) **Administrator Danych Osobowych** – należy przez to rozumieć Miejski Ośrodek Pomocy Społecznej w Wąbrzeźnie reprezentowany przez Dyrektora Jednostki;
2) **Inspektor Ochrony Danych** – należy przez to rozumieć osobę powołaną przez Dyrektora;
3) **Organ nadzorczy** – należy przez to rozumieć Urząd Ochrony Danych Osobowych;
4) **Jednostce** – należy przez to rozumieć Miejski Ośrodek Pomocy Społecznej w Wąbrzeźnie;
5) **Dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
6) **Osoba fizyczna** – osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
7) **Incydent bezpieczeństwa danych osobowych** – należy przez to rozumieć zdarzenie, którego bezpośrednim lub pośrednim skutkiem jest lub może być naruszenie ochrony danych osobowych;
8) **Naruszenie ochrony danych osobowych** – należy rozumieć „naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych” (art. 4 pkt 12 RODO).
9) **Poufność** – należy przez to rozumieć zapewnienie, że dane osobowe nie są udostępniane ani ujawniane podmiotom do tego nieuprawnionym;
10) **Integralność** – zapewnienie, że dane osobowe nie zostały zmienione lub zniszczone przez podmioty do tego nieuprawnione.
11) **Rozliczalność** – zapewnienie, że dane osobowe są przetwarzane w sposób zgodny z prawem oraz wykazanie przestrzegania.

§ 2.
Cel procedury

Celem procedury jest określenie sposobu postępowania w przypadku wystąpienia naruszenia ochrony danych osobowych.

§ 3.
Odpowiedzialność

Odpowiedzialność za określenie wielkości ryzyka naruszenia praw i wolności podmiotów, których naruszenie dotyczy oraz podjęcie działań korygujących spoczywa na Administratorze Danych Osobowych, który przy pomocy Inspektora Ochrony Danych lub osoby wyznaczonej przez Administratora Danych Osobowych, dokonują oceny naruszenia.

§ 4.
Postępowanie w przypadku naruszenia ochrony danych osobowych

W momencie uzyskania informacji o wystąpieniu naruszenia ochrony danych osobowych, ocenia się zastałą sytuacje oraz podejmuje działania mające na celu zminimalizowanie wpływu naruszenia na dane osobowe.

§ 5.

1. Do czasu oceny naruszenia zgłaszający:
   1) powstrzymuje się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności mogących spowodować zatarcie lub naruszenie śladów bądź innych dowodów;
   2) zabezpiecza elementy sprzętu komputerowego lub dokumentacji, przede wszystkim poprzez uniemożliwienie dostępu do nich osobom nieupoważnionym;
   3) podejmuje, stosownie do zaistniałej sytuacji, wszelkie niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.
2. Postanowienia ust. 1 mają zastosowanie zarówno w przypadku naruszenia, jak i w przypadku podejrzenia naruszenia ochrony danych.

§ 6.

W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych osoba oceniająca naruszenie po przybyciu na miejsce:

1) ocenia zastałą sytuację, biorąc pod uwagę w szczególności stan pomieszczeń, w których przetwarzane są dane oraz stan urządzeń, a także identyfikuje wielkość negatywnych następstw incydentu;
2) wysłuchuje relacji osoby, która dokonała powiadomienia;
3) podejmuje decyzje o toku dalszego postępowania, stosownie do zakresu naruszenia lub zasadności podejrzenia naruszenia ochrony danych osobowych.

§ 7.

Z przebiegu zdarzenia, sporządza się sprawozdanie, w którym znajdują się w szczególności informacje o:

1) dacie i godzinie powiadomienia;
2) godzinie pojawienia się w pomieszczeniach, w których przetwarzane są dane;
3) sytuacji, jaką zastał;
4) podjętych działaniach i ich uzasadnieniu.

§ 8.

1. Podejmuje się kroki zmierzające do likwidacji naruszeń zabezpieczeń danych osobowych i zapobieżenia wystąpieniu ich w przyszłości. W tym celu:
   1) w miarę możliwości przywraca stan zgodny z zasadami zabezpieczenia systemu;
   2) o ile taka potrzeba zachodzi, postuluje wprowadzenie nowych form zabezpieczenia, a w razie ich wprowadzenia nadzoruje zaznajamianie z nimi osób zatrudnionych przy przetwarzaniu danych osobowych.

   W przypadku, gdy naruszenie ochrony danych osobowych jest wynikiem uchybienia obowiązującej dyscypliny pracy Inspektor Ochrony Danych Osobowych przekazuje stosowne informacje do Administratora Danych Osobowych, który podejmuje stosowne działania wobec osób, które dopuściły się tego uchybienia.

§ 9.

W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, użytkownik może kontynuować pracę dopiero po otrzymaniu pozwolenia od osoby badającej naruszenie.

§ 10.
Naruszenie praw i wolności osób, których dane osobowe są przetwarzane

1. Administrator Danych Osobowych dokonuje oceny ryzyka czy wystąpienie naruszenia wiąże się z ryzykiem naruszenia praw lub wolności osób fizycznych.
2. Naruszeniem praw i wolności osób, których dane dotyczą będzie m. in.:
   1) powstanie uszczerbku fizycznego;
   2) powstanie szkód majątkowych lub niemajątkowych u osób fizycznych takich jak:
      a) utrata kontroli nad własnymi danymi osobowymi lub ograniczenie praw,
      b) dyskryminacja,
      c) kradzież lub sfałszowanie tożsamości,
      d) strata finansowa,
      e) nieuprawnione odwrócenie pseduonimizacji,
      f) naruszenie dobrego imienia,
      g) naruszenie poufności danych osobowych chronionych tajemnicą zawodową,
      h) wszelkie inne znaczne szkody gospodarcze lub społeczne.

§ 11.
Ocena ryzyka

1. Osoba wyznaczona przez Administratora Danych Osobowych dokonuje oceny ryzyka wpływu naruszenia na prawa i wolności osób, których dane dotyczą.
2. Główne kryteria brane pod uwagę przy ocenie stopnia nasilenia naruszenia danych osobowych:
   1) **Kontekst Przetwarzania Danych (K)** – okoliczności w jakich Administrator Danych Osobowych przetwarza dane;

2) **Łatwość Identyfikacji (I)** – jak łatwo zidentyfikować daną osobę za pomocą naruszonych danych;
3) **Okoliczności Naruszenia (O)** – w jakich okolicznościach nastąpiło naruszenie danych osobowych.

§ 12.
Kontekst Przetwarzania Danych (K)

Aby określić wynik dla Kontekstu Przetwarzania Danych, osoba wyznaczona przez Administratora Danych Osobowych postępuje zgodnie z następującymi krokami:
1) **Krok 1** – Zdefiniowanie i klasyfikacja rodzajów danych osobowych
2) **Krok 2** – Dostosowanie czynników kontekstowych związanych z przetwarzaniem danych (ocena okoliczności występowania pewnych czynników, które mogłyby zwiększyć lub zmniejszyć punktację podstawową).

§ 13.
Identyfikacja i klasyfikacja rodzajów danych osobowych

1. Podmiot wyznaczony przez Administratora Danych osobowych zidentyfikował i sklasyfikował następujące kategorie danych osobowych i odpowiadające im punkty kontekstowe:
   1) **Dane proste** (dane kontaktowe, imię, nazwisko, dane dotyczące edukacji, życia rodzinnego, doświadczenia zawodowego, dane biograficzne itp.)

Okoliczność	Punkty
Wstępny wynik podstawowy: kiedy naruszenie obejmuje dane proste, a Administrator nie jest świadomy żadnych czynników obciążających	**1**
Wynik zostaje zwiększony o 1, np. gdy objętość „prostych danych" i / lub cechy pozwalają na profilowanie poszczególnych osób, lub można uzyskać założenia dotyczące statusu społeczno-finansowego.	2
Wynik zostaje zwiększony o 2, gdy „dane proste" pozwalają na uzyskanie założenia stanu zdrowia, preferencje seksualne, przekonania polityczne lub religijne.	3
Wynik zostaje zwiększony o 3, gdy pewne cechy charakterystyczne osoby (np. grupy wrażliwe, małoletni) mogą być kluczowe dla ich osobistego bezpieczeństwa lub warunków fizycznych / psychologicznych.	4

   2) **Dane behawioralne** (lokalizacja, dane o ruchu, personalne preferencje, nawyki itp.)

Okoliczność	Punkty
Wstępny wynik podstawowy: jeśli naruszenie obejmuje dane behawioralne, a Administrator nie jest świadomy żadnych czynników obciążających	**2**

Wynik zostaje zmniejszony o 1, gdy natura zbioru danych nie dostarcza istotnych informacji o zachowaniu użytkownika, a dane mogą być zbierane łatwo (niezależnie od naruszenia) za pośrednictwem publicznie dostępnych źródeł (np. połączenie informacji z wyszukiwarek internetowych dotyczące osoby, której dane zostały naruszone)	1
Wynik zostaje zwiększony o 1, jeżeli objętość danych behawioralnych i / lub cech przetwarzanych przez Administratora pozwalają na stworzenie profilu osoby, ujawniając szczególne informacje o swoim życiu codziennym i nawykach	3
Wynik zostaje zwiększony o 2, jeżeli może zostać utworzony profil zawierający dane wrażliwe	4

3) **Dane finansowe** (np. dochody, transakcje finansowe, wyciągi bankowe, faktury itp.)

Okoliczność	Punkty
Wstępny wynik podstawowy: jeśli naruszenie obejmuje dane finansowe, a Administrator nie jest świadomy żadnych czynników obciążających	**3**
Wynik zostaje zmniejszony o 2, jeżeli natura zbioru nie dostarcza istotnych informacji finansowych danej osoby (np. fakt, że dana osoba jest klientem danego banku)	1
Wynik zostaje zmniejszony o 1, np. gdy konkretny zestaw danych zawiera pewne informacje finansowe, ale nadal nie dostarcza istotnych informacji na temat sytuacji finansowej / życiowej (np. numery kont bankowych bez dodatkowej informacji)	2
Wynik zostaje zwiększony o 1, gdy ze względu na charakter i / lub objętość określonego zbioru danych, umożliwia stworzenie szczegółowego profilu społeczno-finansowego osoby, której dane dotyczą	4

4) **Dane szczególnej kategorii** (dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne, zdrowia, seksualności lub orientacji seksualnej, wyroków skazujących).

Okoliczność	Punkty
Wstępny wynik podstawowy: jeśli naruszenie obejmuje dane wrażliwe, a Administrator nie jest świadomy żadnych czynników obciążających	**4**
Wynik może zostać zmniejszony o 3, np. gdy natura zbioru nie dostarcza istotnych informacji o zachowaniu osób, których dane zostały naruszone, a dane mogą zostać łatwo zebrane (niezależnie od naruszenia) za pośrednictwem publicznie dostępnych źródeł (np. połączenie informacji z wyszukiwarek internetowych)	1
Wynik może zostać zmniejszony o 2, np. gdy charakter danych może prowadzić wyłącznie do ogólnych założeń	2
Wynik może zostać zmniejszony o 1, np. gdy natura danych może prowadzić wyłącznie do założeń dotyczących poufnych informacji	3

2. W momencie, kiedy naruszeniu ulegają dane wielu kategorii, jako wynik Kontekstu Przetwarzania Danych (K) wykorzystujemy najwyższy wynik.

§ 14.
Łatwość Identyfikacji (I)

1. Łatwość Identyfikacji jest definiowana na jednym z czterech poziomów:
   1) **I = 0,25** (poziom nieistotny), np. w przypadku: imienia i nazwiska, które występują znacznie w skali całego kraju; numeru paszportu nie powiązanego z żadnymi dodatkowymi informacjami umożliwiającymi wykorzystanie danej w kontekście; adresu poczty elektronicznej, którego nazwa nie zdradza żadnych dodatkowych danych o osobie, której dane dotyczą; nieostre zdjęcie.
   2) **I = 0,5** (poziom ograniczony), np. w przypadku: imienia i nazwiska, które występują rzadko w skali całego kraju; numeru telefonu, gdzie identyfikacja jest możliwa poprzez bezpośrednią komunikację; zdjęcia, które jest nieostre ale umożliwia identyfikację miejsca w którym zostało zrobione.
   3) **I = 0,75** (poziom znaczący), np. w przypadku: imienia i nazwiska, które występują rzadko w skali danego miasta; numeru PESEL, który umożliwia uzyskanie informacji o dacie urodzenia; adresu poczty elektronicznej, którego nazwa wskazuje na imię i nazwisko, ale dzięki któremu nie da się uzyskać dodatkowych informacji poprzez wyszukiwarki internetowe; zdjęcia wysokiej jakości, które jednak nie wskazuje na okoliczności wykonania zdjęcia poprzez np. unikatowość miejsca, w którym zostało zrobione.
   4) **I = 1** (poziom maksymalny), np. w przypadku: imienia i nazwiska, które w połączeniu z datą urodzenia jednoznacznie wskażą daną osobę; numeru PESEL uzyskanego razem z imieniem i nazwiskiem; numeru telefonu, który jest zarejestrowany w ogólnodostępnym rejestrze; adresie poczty elektronicznej, którego nazwa wskazuje na dodatkowe dane takie jak imię, nazwisko oraz może posłużyć do uzyskania dodatkowych informacji za pośrednictwem wyszukiwarek internetowych; zdjęcia

wysokiej rozdzielczości, które umożliwia identyfikację osoby na nim się znajdującej wraz z miejscem w którym zostało zrobione, lub okolicznościami wykonania zdjęcia.

2. W momencie, kiedy naruszeniu ulegają dane wielu kategorii, jako wynik Łatwości Identyfikacji (I) wykorzystujemy najwyższy wynik.

§ 15.
Okoliczności Naruszenia (O)

Elementami analizowanymi w ramach określania Okoliczności Naruszenia jest utrata bezpieczeństwa (**poufność, integralność, dostępność**) oraz złego zamiaru i uzupełniają Kontekst Przetwarzania Danych i Łatwość Identyfikacji w następujący sposób:

1) **Utrata poufności** (występuje wtedy, gdy informacje są dostępne dla stron, które są nieupoważnione lub nie maja prawnie do tego celu dostępu)

Naruszenie danych bez zaistnienia dowodów na nielegalne przetwarzanie	0
Udostępnienie danych znanej liczbie określonej odbiorców	+ 0,25
Udostępnienie danych nieznanej ilości odbiorów	+ 0,5

2) **Utrata integralności** (występuje wtedy, gdy oryginalne dane są zmienione i podstawione)

Zmiana danych bez zidentyfikowanego nieprawidłowego lub nielegalnego użycia	0
Zmiana danych wraz z możliwością ich nieprawidłowego lub nielegalnego wykorzystania, ale przy możliwości odzyskania oryginalnych informacji	+ 0,25
Zmiana danych wraz z możliwością ich nieprawidłowego lub nielegalnego użycia, bez możliwości odzyskania oryginalnych informacji	+ 0,5

3) **Utrata dostępności** (występuje wtedy, gdy nie można uzyskać oryginalnych danych, wtedy, gdy istnieje do dostępu potrzeba. Może to być czasowe lub trwałe)

Utrata danych, możliwych do odzyskania bez żadnych trudności	0
Tymczasowa niedostępność danych	+ 0,25
Kompletna niedostępność (bez możliwości odzyskania danych)	+ 0,5

§ 16.
Obliczanie ciężkości

1. Obliczanie wysokość poziomu ryzyka dla praw i wolności osób, których dane dotyczą, podmiot wyznaczony należy skorzystać z następującego wzoru:

$$R = K \times I + O$$

Poziom Ryzyka = Kontekst Przetwarzania Danych x Łatwość Identyfikacji + Okoliczności Naruszenia

2. Podmiot wyznaczony przez Administratora Danych Osobowych dokonuje oceny ryzyka wpływu naruszenia na prawa i wolności osób, których dane dotyczą.
3. Końcowy wynik pokazuje poziom ciężkości danego naruszenia.

Poziom ryzyka wpływu naruszenia na prawa i wolności, których dane dotyczą		
$R < 2$	**Mały**	Osoby, których dane zostały naruszone nie odczują tego skutku, bądź spotkają się z nielicznymi niedogodnościami, nie stanowiącymi większego problemu (np. czas poświęcony na ponowne wprowadzenie danych, rozdrażnienie, irytacja)
$2 \leq R < 4$	**Średni**	Osoby, których dane zostały naruszone mogą napotkać znaczne niedogodności, które będą w stanie pokonać pomimo kilku trudności (np. dodatkowe koszty, niemożność korzystania z usług biznesowych, strach, brak zrozumienia, stres, dolegliwości fizyczne itp.)
$4 \leq R$	**Wysoki**	Osoby, których dane zostały naruszone mogą napotkać znaczne, konsekwencje, których nie mogą pokonać (trudności finansowe, takie jak czarne listy banków, dług, szkody materialne lub niemożność pracy, długoterminowe dolegliwości psychologiczne, itp.)

§ 17.
Notyfikacja organu nadzorczego

1. Jeżeli po przeprowadzonej ocenie, istnieje ryzyko naruszenia praw i wolności osób fizycznych, Administrator Danych zawiadamia niezwłocznie organ nadzorczy, jednak nie później niż w ciągu 72 godzin po stwierdzeniu naruszenia.
2. Zgłoszenie naruszenia przez Administratora Danych następuje poprzez wypełnienie dedykowanego formularza dostępnego na stronie internetowej Organu nadzorczego oraz wysłanie formularza na jeden z poniższych sposobów.:
   a) Elektronicznie poprzez wypełnienie dedykowanego formularza dostępnego bezpośrednio na platformie biznes.gov.pl
   b) Elektronicznie poprzez wysłanie wypełnionego formularza na elektroniczną skrzynkę podawczą ePUAP: UODO/SkrytkaESP
   c) Elektronicznie poprzez wysłanie wypełnionego formularza za pomocą pisma ogólnego dostępnego na platformie biznes.gov.pl,
   d) Tradycyjną pocztą, wysyłając wypełniony formularz na adres Urzędu.
3. Wzór zgłoszenia naruszenia ochrony danych osobowych według obowiązującego wzoru na stronie internetowej organu nadzorczego.
4. W przypadku przekroczenia terminu wskazanego w ust. 1 w zgłoszeniu należy dołączyć wyjaśnienie przyczyny opóźnienia zgodnie z obowiązującym wzorem zgłoszenia naruszenia ochrony danych osobowych dostępnego na stronie internetowej organu nadzorczego.
5. Jeżeli w przypadku wejścia w posiadanie nowych informacji nastąpiła zmiana opisywanej sytuacji lub administrator zastosował dodatkowe środki, administrator zgłasza bez zbędnej zwłoki wszystkie nowe informacji organowi nadzorczemu.

6. Administrator danych dokumentuje wszystkie naruszenia ochrony danych, w tym jego okoliczności, skutki oraz podjęte działania zaradcze, zgodnie **z wzorem nr 3.**
7. Rejestr naruszeń prowadzony jest w formie elektronicznej oraz papierowej.

§ 18.
Zawiadomienie osób fizycznych, których dane zostały naruszone

1. Jeżeli po przeprowadzonej ocenie, poziom ryzyka wpływu naruszenia na prawa i wolności osób, których dane zostały naruszone został określony jako wysoki, Administrator Danych prostym i jasnym językiem zawiadamia bez zbędnej zwłoki osoby, których dane osobowe zostały naruszone.
2. W zależności od ilości osób, których dane zostały naruszone, Administrator Danych Osobowych zawiadamia podmioty, których dane dotyczą poprzez:
   1) Pisemnie, korespondencyjnie, na znany nam adres podmiotu (wzór pisemnego zgłoszenia określa **wzór nr 1**);
   2) W przypadku braku możliwości korespondencyjnego zawiadomienia, Administrator Danych Osobowych wykorzystuje posiadane możliwości zawiadomienia (np. telefonicznie, drogą elektroniczną);
   3) Wydanie publicznego komunikatu (wzór publicznego komunikatu określa **wzór nr 2)**

§ 19.
Działania zaradcze

Administrator Danych Osobowych wyznacza osobę do podjęcia działań zaradczych w celu zmniejszenia ryzyka ponownego wystąpienia naruszenia ochrony danych osobowych.

Wzór nr 1 do Procedury postępowania w przypadku naruszenia ochrony danych osobowych w MOPS Wąbrzeźno

……..
(miejscowość, data)

Administrator danych
Ul. ……..
//-//// ……..

Do:
. . . . . .
. . . . . .
. . . . . .

ZGŁOSZENIA W SPRAWIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Zgodnie z art. 34 ogólnego rozporządzenia o ochronie danych, zgłaszam naruszenie ochrony danych osobowych, które miało miejsce w dniu . . . . . w . . . . . .

Zgłoszenie te ma na celu umożliwienie podjęcia niezbędnych działań zapobiegawczych w celu minimalizacji potencjalnych niekorzystnych skutków naruszenia.

1.	Charakter naruszenia ochrony danych:	
3.	Kategoria danych osobowych, które uległy naruszeniu:	
4.	Możliwe konsekwencje naruszenia ochrony danych:	
5.	Zalecenia co do minimalizacji potencjalnych niekorzystnych skutków:	
6.	W celu uzyskania dodatkowych wyjaśnień, proszę o kontakt z:	

……
(czytelny podpis Administratora Danych)

Wzór nr 2 do Procedury postępowania w przypadku naruszenia ochrony danych osobowych w MOPS Wąbrzeźno

ZGŁOSZENIA W SPRAWIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Zgodnie z art. 34 ogólnego rozporządzenia o ochronie danych, informuję iż doszło do naruszenia ochrony danych osobowych, które miało miejsce w dniu . . . . . w . . . . . .

Zgłoszenie te ma na celu umożliwienie podjęcia niezbędnych działań zapobiegawczych w celu minimalizacji potencjalnych niekorzystnych skutków naruszenia.

Charakter naruszenia miał postać . . . . . .

Naruszeniu ochrony danych osobowych uległy dane . . . . . (określić kategorię osób, których dane uległy naruszeniu wraz z kategoriami danych osobowych).

Możliwymi konsekwencjami zaistniałego naruszenia są . . . . . .

W celu zminimalizowania potencjalnych skutków naruszenia zaleca się . . . . . .

W celu uzyskania dodatkowych wyjaśnień, proszę o kontakt z:

……
(czytelny podpis Administratora Danych)

Wzór nr 3 do Procedury postępowania w przypadku naruszenia ochrony danych osobowych w MOPS Wąbrzeźno

REJESTR NARUSZEŃ OCHRONY DANYCH OSOBOWYCH

Lp.	Data wystąpienia naruszenia	Rodzaj naruszenia	Kategoria osób, których dane zostały naruszone wraz z kategorią naruszonych danych osobowych	Okoliczności naruszenia	Skutki naruszenia