ZARZĄDZENIE Nr 7/2022
KIEROWNIKA OŚRODKA POMOCY SPOŁECZNEJ W STARYM SĄCZU
z dnia 7 lipca 2022 r.

w sprawie wprowadzenia Procedury postępowania w sytuacji naruszenia ochrony danych osobowych w Ośrodku Pomocy Społecznej w Starym Sączu.

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 osobowych), **zarządzam co następuje**:

§1. Wprowadzam w w Ośrodku Pomocy Społecznej w Starym Sączu „Procedurę postępowania w sytuacji naruszenia ochrony danych osobowych w Ośrodku Pomocy Społecznej w Starym Sączu", zwanej dalej Procedurą, w brzmieniu stanowiącym załącznik do niniejszego zarządzenia.

§2. Zobowiązuję wszystkich pracowników Ośrodka Pomocy Społecznej w Starym Sączu do zapoznania się z treścią Procedury.

§3. Zobowiązuję wszystkich pracowników do przestrzegania i stosowania zasad postępowania określonych w Procedurze.

§4. W procedurze "Polityka Bezpieczeństwa Informacji Ośrodka Pomocy Społecznej w Starym Sączu przyjętej Zarządzeniem Nr 7/2018 Kierownika Ośrodka Pomocy Społecznej w Starym Sączu z dnia 28.05.2018 r. uchyla się załącznik 11 - Rejestr incydentów i naruszeń bezpieczeństwa".

§5. Zarządzenie wchodzi w życie z dniem podpisania.

Franciszek Tudaj
Kierownik Ośrodka Pomocy Społecznej
w Starym Sączu

Załącznik do Zarządzenia Nr 7/2022
Kierownika Ośrodka Pomocy Społecznej w Starym Sączu z dnia 7.07.2022 r.

Procedura postępowania w sytuacji naruszenia ochrony danych osobowych w Ośrodku Pomocy Społecznej w Starym Sączu

I. Istota naruszenia ochrony danych osobowych

§1.1.Incydentem w zakresie danych osobowych jest sytuacja powodująca utratę poufności, integralności lub dostępności przetwarzanych danych osobowych.

1) poufność – właściwość polegająca na tym, że informacja nie jest udostępniania ani ujawniana nieautoryzowanym osobom, podmiotom lub procesom;
2) integralność – właściwość polegająca na zapewnieniu dokładności i kompletności;
3) dostępność – właściwość polegająca na byciu dostępnym i użytecznym na żądanie autoryzowanego podmiotu.

2. Naruszeniem danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:
1) nieautoryzowany dostęp do danych;
2) nieautoryzowana modyfikacja lub zniszczenie danych;
3) udostępnienie danych nieautoryzowanym podmiotom;
4) nielegalne ujawnienie danych;
5) pozyskanie danych z nielegalnym źródeł.

II. Postępowanie w sytuacji naruszenia ochrony danych osobowych

§2.1. Każdy pracownik, osoba upoważniona do przetwarzania danych osobowych w Ośrodku Pomocy Społecznej w Starym Sączu zobowiązana jest do niezwłocznego powiadomienia w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych swojego bezpośredniego przełożonego. Przełożony zgłasza fakt Inspektorowi Ochrony Danych .
2. Do sytuacji wymagających powiadomienia i reakcji należą:
1) ślady na drzwiach, oknach, szafach wskazujących na próbę włamania;
2) niewłaściwe niszczenie dokumentacji, bez użycia niszczarek;
3) obecność w budynku lub pomieszczeniu osób zachowujących się podejrzanie;
4) pozostawione otwarte drzwi do pomieszczeń, szaf, miejsc, gdzie przechowywane są dane osobowe;
5) ustawienie monitorów, które pozwala na wgląd osób postronnych w dane osobowe;
6) wynoszenie danych osobowych w wersji papierowej lub elektronicznej na zewnątrz Urzędu bez stosownego upoważnienia;
7) udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej lub ustnej;
8) telefoniczne próby wyłudzenia danych osobowych;
9) kradzież, zagubienie komputerów, CD, twardych dysków, pen-drive z danymi osobowymi;
10) maile z nieznanych źródeł zachęcające do ujawnienia danych, identyfikatorów i/lub haseł;
11) pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów;
12) przechowywanie w pobliżu komputerów, w miejscach łatwo dostępnych haseł do systemów;
13) brak stosowania zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka, czystego ekranu, czystej drukarki);
14) zdarzenia losowe zewnętrzne mające istotny wpływ na bezpieczeństwo danych osobowych (np. pożar budynku, pomieszczenia, zalanie wodą, długotrwała utrata zasilania lub łączności);

15) zdarzenie losowe wewnętrzne mające istotny wpływ na bezpieczeństwo danych osobowych (np. awarie serwera, komputerów, pomyłki pracowników, zagubienie danych);
16) umyślne incydenty (świadome zniszczenie dokumentów, działanie wirusa lub innego szkodliwego oprogramowania).

§3. Każdy pracownik, który stwierdzi fakt naruszenia ochrony danych osobowych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz zabezpieczyć dowody umożliwiające ustalenie przyczyny oraz skutki naruszenia.

§4. W przypadku stwierdzenia naruszenia bezpieczeństwa danych należy natychmiast zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej przyczyny miejsca zdarzenia do czasu przybycia przełożonego, Inspektora Ochrony Danych lub innej upoważnionej przez Administratora osoby.

§5. Administrator Systemów Informatycznych zobowiązany jest do ścisłego współdziałania z Inspektorem Ochrony Danych w sytuacji, gdy naruszenie dotyczy systemów informatycznych oraz do podjęcia natychmiastowych działań zapobiegawczych i naprawczych.

§6. Inspektor Ochrony Danych podejmuje następujące działania:

1. zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości i ciągłości pracy,
2. odbiera dokładną relację od osoby powiadamiającej, oraz od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem,
3. jeśli zachodzi taka konieczność nawiązuje kontakt ze specjalistami (podmiotami) zewnętrznymi.

§ 7. Inspektor Ochrony Danych dokumentuje zaistniałą sytuację naruszającą bezpieczeństwo danych sporządzając Raport – stanowi **Załącznik Nr 1** do Procedury oraz rejestruje naruszenie w Rejestrze Naruszeń stanowiącym **Załącznik nr 2** do Procedury.

III. Naruszenie ochrony danych osobowych - odpowiedzialność

§ 8. Wobec osoby, która w przypadku naruszenia ochrony danych osobowych nie podjęła działania określonego w niniejszej Procedurze, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, pracodawca może wszcząć postępowanie dyscyplinarne lub porządkowe. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych. Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z obowiązującymi przepisami prawa oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

IV. Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu – Prezesowi Urzędu Ochrony Danych Osobowych

§ 9. 1. Organem właściwym, któremu dokonuje się zgłoszenia naruszeń ochrony danych osobowych jest Prezes Urzędu Ochrony Danych Osobowych.
Zgłoszenia dokonuje Administrator bez zbędnej zwłoki, w miarę możliwości nie później niż 72 godziny po stwierdzeniu naruszenia, chyba że jest mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Zgłoszenia można dokonać na 4 sposoby:
1) elektronicznie poprzez wypełnienie dedykowanego formularza elektronicznego dostępnego bezpośrednio na platformie biznes.gov.pl .
2) elektronicznie poprzez wysłanie wypełnionego formularza na elektroniczną skrzynkę podawczą

ePUAP: /UODO/SkrytkaESP.
3) elektronicznie poprzez wysłanie wypełnionego formularza za pomocą pisma ogólnego dostępnego na platformie biznes.gov.pl lub platformie epuap.gov.pl.
4) tradycyjną pocztą wysyłając wypełniony formularz – wzór określony w **Załączniku Nr 3** do Procedury - na adres Urzędu Ochrony Danych Osobowych (ul. Stawki 2, 00 - 193 Warszawa).

2. W zgłoszeniu należy w szczególności:
1) opisać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
2) wskazać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych;
3) opisać możliwe konsekwencje naruszenia ochrony danych osobowych;
4) opisać środki zastosowane lub proponowane w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

3. Jeżeli informacji, o których mowa w ust. 2, nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki w następujący sposób:
1) po dokonaniu pierwszego zgłoszenia można przekazywać na bieżąco organowi nadzorczemu aktualne informacje;
2) w przypadku uzyskania w toku dochodzenia dowodów na to, że opanowano zdarzenie, a w rzeczywistości żadne naruszenie nie miało miejsca, informację tę można dodać do informacji już przekazanych do organu nadzorczego, a następnie zarejestrować zaistniałe zdarzenie jako niestanowiące naruszenia ochrony danych osobowych.

4. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

V. Postępowanie w sytuacji stwierdzenia, że naruszenie ochrony danych osobowych stanowi zdarzenie o charakterze przestępczym

§10.1 Ocena charakteru naruszenia w kontekście możliwości naruszenia przepisów prawa.

2. Inspektor Ochrony Danych w porozumieniu z Administratorem Systemów Informatycznych, jeśli zdarzenie dotyczy systemów informatycznych, dokonuje wstępnej oceny charakteru naruszenia w zakresie możliwości uznania, że stanowi ono działanie o charakterze przestępczym, a następnie niezwłocznie przekazuje Administratorowi wszelkie informacje związane z tym naruszeniem.

3. Na ocenę charakteru naruszenia, nie ma wpływu, czy jest to naruszenie zamierzone, czy nie zamierzone, ani to czy jest to naruszenie o charakterze wewnętrznym lub zewnętrznym.

4. Inspektor Ochrony Danych w porozumieniu z Administratorem System Informatycznych oraz Administratorem dokonują oceny charakteru naruszenia, uwzględniając:
1) intencje osoby lub osób, które doprowadziły do naruszenia;
2) skutki naruszenia dla osób, których dane dotyczą;
3) skutki naruszenia dla organizacji administratora;
4) spełnienie przesłanek popełnienia czynu zabronionego, o których mowa w Kodeksie karnym;
5) obowiązki administratora wynikające z przepisów szczególnych w związku z naruszeniem;
6) w szczególności obowiązek zawiadomienia organów ścigania.

5. Naruszeniami ochrony danych osobowych, które uznaje się za zdarzenia o charakterze przestępczym będą w szczególności:
1) kradzież danych osobowych lub urządzeń z danymi osobowymi;
2) umyślne usunięcie lub zniszczenie danych osobowych;
3) zaszyfrowanie danych osobowych na skutek działania złośliwego oprogramowania;
4) podszywanie się pod pracownika lub w celu wyłudzenia danych;
5) umyślne zniszczenie urządzeń, na których przetwarzane są dane osobowe;

6) umyślne wykorzystanie danych osobowych klientów Urzędu/pracowników w celu wzięcia pożyczki na ich dane;
7) żądanie okupu za wykradzione lub zaszyfrowane dane osobowe;
8) grożenie administratorowi usunięciem/kradzieżą/zniszczeniem danych osobowych;
9) sprzedaż skradzionych danych innym podmiotom.

6. Przykłady wskazane w punkcie wcześniejszym nie stanowią katalogu zamkniętego.
7. W przypadku stwierdzenia, że naruszenie ma charakter przestępczy, należy niezwłocznie powiadomić o tym Administratora oraz sporządzić Raport z dokonanej oceny charakteru naruszenia.

§11.1 Zgłoszenie zdarzenia do organów ścigania

2. Decyzję o zgłoszeniu naruszenia do organów ścigania podejmuje Administrator lub upoważnione przez niego w tym zakresie osoby.
3. Administrator powinien dokonać zgłoszenia niezwłocznie, gdyż czas reakcji może mieć istotny wpływ na możliwość podjęcia skutecznych działań przez organy ścigania.
4. Informację o zawiadomieniu organów ścigania należy udokumentować i przechowywać wraz z innymi informacjami dokumentującymi naruszenie ochrony danych.
5. Zawiadomienie organów ścigania o naruszeniu, pozostaje bez wpływu na obowiązki administratora, związane ze zgłoszeniem naruszenia, wynikające z art. 33 RODO.
6. W przypadku zawiadomienia organów ścigania o naruszeniu, należy poinformować o tym organ nadzorczy. Jeżeli zgłoszenie naruszenia zostało przekazane przed zawiadomieniem organów ścigania, należy przesłać zgłoszenie uzupełniające.
7. Administrator postępuje zgodnie z poleceniami organów ścigania i współpracuje z nimi, w szczególności w zakresie ujawniania lub nieujawniania informacji o naruszeniu, w tym niezwłocznego zawiadamiania lub opóźnienia zawiadamiania osób, których dotyczy naruszenie, jeżeli takie działanie może mieć wpływ na prowadzone postępowanie.

VI. Zawiadomienie osoby, której dane dotyczą o naruszeniu ochrony danych osobowych

§12.1 Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki zawiadamia o tym osoby, których dane dotyczą.

2. Zawiadomienie należy przygotować jasnym i prostym językiem z uwzględnieniem wymogów określonych w art.33 ust.3 lit. b),c) i d) RODO. Wzór zawiadomienia określa **Załącznik nr 4** do Procedury.

3. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane w następujących przypadkach:
   1) Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
   2) Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
   3) zawiadomienie wymagałoby niewspółmiernie dużego wysiłku; w takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

4. Należy wykazać przed organem nadzorczym, że został spełniony przynajmniej jeden z warunków wskazanych w ust.3 w przypadku braku powiadomienia osób, których dane naruszono.

Raport znaruszenia ochrony danych osobowych

1. Data sporządzenia Raportu…….. godzina …….

2. Osoba powiadamiająca o naruszeniu …….. ……
(imię, nazwisko, stanowisko)

3. Inne osoby udzielające informacji i wyjaśnień …….. ……

4. Miejsce, dokładny czas i data naruszenia ochrony danych osobowych (piętro, nr pokoju, godzina, nazwa programu, aplikacji, itp.):
.....
.....

5. Rodzaj naruszenia i okoliczności towarzyszące naruszeniu, w tym przyczyna naruszenia…….
.....
.....
.....

6. Kategorie danych, których dotyczy naruszenie:
.....

7. Kategorie osób, których dotyczy naruszenie:
.....

8. Podjęte działania wyjaśniające i naprawcze.....
.....
.....

…….. (podpis pracownika)

……. (data i podpis IOD)

……. (podpis Administratora)

Zatwierdzam wzór ……

Rejestr naruszeń i incydentów ochrony danych osobowych

Lp.	Data / godzina naruszenia	Kategoria osób, których dane zostały naruszone	Kwalifikacja naruszenia (niskie lub wysokie)	Zastosowa-ne środki zaradcze	Zgłoszenie do organu nadzorczego (dotyczy lub nie dotyczy)	Zawiadomienie osoby której dane dotyczą (dotyczy lub nie dotyczy)
1.						
2.						
3.						
4.						
……						

Zatwierdzam wzór

……

Zgłoszenie o naruszeniu ochrony danych osobowych organowi nadzorczemu

_____ , _____
(miejscowość) (data)

Nazwa Jednostki …….

adres (dane korespondencyjne):

…….

…….

Prezes Urzędu Ochrony Danych Osobowych
Urząd Ochrony Danych Osobowych
ul. Stawki 2
00-193 Warszawa

Zgłoszenie naruszenia ochrony danych osobowych

Na podstawie obowiązku wynikającego z art. 33 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 - RODO).

Data naruszenia	
Liczba osób których dane dotyczą	
Liczba wpisów danych osobowych i kategoria tych danych	
Dane Inspektora Danych osobowych	
Dane Organu Nadzorczego	
Charakter Naruszenia	
Konsekwencje naruszenia	

Zastosowane i proponowane środki zaradcze	

……
(Podpis Administratora)

Zatwierdzam wzór …….

Zawiadomienie o naruszeniu ochrony danych osoby, której dane zostały naruszone

_____ , _____
(miejscowość) (data)

Nazwa Jednostki …….

Adres:

…….

Sz. P.

…….

Zawiadomienie o naruszeniu ochrony danych osobowych

Na podstawie obowiązku wynikającego z art. 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 - RODO) w związku z naruszeniem Pana/Pani danych osobowych w zakresie ……. zawiadamiamy co następuje:

Konsekwencją wyżej wymienionej sytuacji jest podjęcie przez osoby nieupoważnione informacji w zakresie……..

Zawiadamiający podjął wszelkie możliwe środki celem minimalizacji skutków naruszenia między innymi: zawiadomienie do organu nadzorczego, zawiadomienie organów ścigania, wcześniejsza szyfryzacja danych.

Celem uzyskania dodatkowych informacji należy kontaktować się z .....

_____
(Podpis Administratora)

Zatwierdzam wzór ……