DOM POMOCY SPOŁECZNEJ
"ZAMECZEK"
44-144 Kuźnia Nieborowska
ul. Knurowska 13, tel. (32) 235 16 30

Kuźnia Nieborowska, 2020-12-30

Zarządzenie wewnętrzne nr 22/2020
Dyrektora Domu Pomocy Społecznej „Zameczek" w Kuźni Nieborowskiej
z dnia 30.12.2020 r.
w sprawie wprowadzenia w życie Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych w Domu Pomocy Społecznej „Zameczek" w Kuźni Nieborowskiej

- Z dniem 30.12.2020 r. wprowadza się Instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych w Domu Pomocy Społecznej „Zameczek" w Kuźni Nieborowskiej.
- Postanowienia w/w Instrukcji obowiązują wszystkie osoby zatrudnione na stanowiskach, na których ma miejsce przetwarzanie danych osobowych.
- Wszystkie osoby zatrudnione na stanowiskach, na których ma miejsce przetwarzanie danych osobowych mają obowiązek zapoznać się z treścią w/w Instrukcji oraz przestrzegać zasad wynikających z w/w dokumentu.
- Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
Domu Pomocy Społecznej "Zameczek"
w Kuźni Nieborowskiej
mgr Ewa Zamora

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH W DOMU POMOCY SPOŁECZNEJ „ZAMECZEK" W KUŹNI NIEBOROWSKIEJ

Terminologia:

1) **Czynność Przetwarzania** – jedna lub więcej czynności w znaczeniu potocznym, obejmująca Przetwarzanie Danych Osobowych w jednym i tym samym celu; kilka czynności w znaczeniu potocznym stanowi jedną Czynność Przetwarzania, jeśli poza wspólnym celem tego Przetwarzania tworzą one pewną funkcjonalną całość (np. prowadzenie akt pracowniczych).
2) **Dane Osobowe** (także: **„Dane"**) – każda informacja o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.
3) **Naruszenie Ochrony Danych Osobowych** - oznacza 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.
4) **Pracownik** – w rozumieniu niniejszego Instrukcji oznacza każą osobę świadczącą dla DPS „Zameczek" pracę lub usługi, bez względu na podstawę takiego świadczenia i mającą w związku z tym styczność z Danymi Osobowymi.
5) **Przetwarzanie Danych Osobowych** (także: **„Przetwarzanie")** – jedna lub więcej czynności wykonywanych na Danych Osobowych (lub ich zestawach), taka jak zbieranie, utrwalanie, porządkowanie, przechowywanie, modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, usuwanie lub niszczenie.
6) **RODO** - rozporządzenie parlamentu europejskiego i rady (UE) 2016/679 z 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).
7) **UODO** – Urząd Ochrony Danych Osobowych, ul. Stawki 2 , 00-193 Warszawa.
8) **Ustawa o ochronie danych osobowych** – Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000).
9) **Udostępnienie Danych** - oznacza ujawnienie Danych podmiotowi trzeciemu.
10) **Upoważnienie do Przetwarzania Danych** – pisemne oświadczenie DPS „Zameczek" wskazujące imiennie osobę upoważniona do Przetwarzania Danych oraz jedną lub więcej Czynności Przetwarzania, które upoważnienie obejmuje.
11) **DPS „Zameczek"** (także: **„Administrator"** oraz **„DPS"**) – Dom Pomocy „Zameczek" w Kuźni Nieborowskiej, reprezentowany przez Dyrektora DPS, występujące w stosunku do przetwarzanych przez siebie Danych Osobowych jako ich administrator, tj. podmiot, który (samodzielnie lub wspólnie z innymi) ustala cele i sposoby Przetwarzania tych Danych

I. ISTOTA NARUSZENIA DANYCH OSOBOWYCH

§1

Incydentem w zakresie Danych osobowych jest sytuacja powodująca utratę poufności, integralności lub dostępności przetwarzanych Danych.

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. nieautoryzowane modyfikacje lub zniszczenie Danych,
3. udostępnienie Danych nieautoryzowanym podmiotom,
4. nielegalne ujawnienie Danych,
5. pozyskiwanie Danych z nielegalnych źródeł.

II. POSTĘPOWANIE W PRZYPADKU NARUSZENIA DANYCH OSOBOWYCH

§2

1. Każdy Pracownik, który stwierdzi lub podejrzewa fakt naruszenia Danych osobowych jest zobowiązany niezwłocznie zgłosić to Dyrektorowi DPS (bądź Inspektorowi Ochrony Danych – dalej IODO bądź swemu bezpośredniemu przełożonemu. Przełożony zgłasza podejrzenie bądź fakt naruszenia Dyrektorowi DPS bądź IODO.
2. Typowe sytuacje, gdy Pracownik powinien powiadomić Dyrektora DPS (bądź IODO):
   a. ślady na drzwiach, oknach i szafach wskazują na próbę włamania;
   b. dokumentacja jest niszczona bez użycia niszczarki;
   c. fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie;
   d. otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są Dane osobowe, stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, płytach CD w formie niezabezpieczonej itp.
   e. niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie Danych w drukarce, na ksero, niezamknięcie pomieszczenia z komputerem, niewykonanie w określonym terminie kopii bezpieczeństwa, prace na

informacjach służbowych w celach prywatnych,

f. ustawienie monitorów pozwala na wgląd osób postronnych w Dane osobowe;
g. wynoszenie Danych osobowych w wersji papierowej lub elektronicznej na zewnątrz firmy bez upoważnienia;
h. udostępnienie Danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej lub ustnej;
i. stwierdzono próbę lub modyfikację Danych lub zmianę w strukturze Danych bez odpowiedniego upoważnienia (autoryzacji),
j. telefoniczne próby wyłudzenia Danych osobowych;
k. kradzież komputerów lub twardych dysków z danymi osobowymi;
l. utrata kontroli nad kopią Danych osobowych;
m. maile zachęcające do ujawnienia identyfikatora i/lub hasła;
n. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów;
o. istnienie nieautoryzowanych kont dostępu do Danych lub tzw. "bocznej furtki"
p. hasła do systemów przechowywane są w pobliżu komputera.

§3

Każdy Pracownik, który stwierdzi fakt naruszenia Danych osobowych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia,

§4

W przypadku stwierdzenia naruszenia bezpieczeństwa Danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Dyrektora DPS (bądź IODO) bądź osoby przez niego upoważnionej.

§5

Dyrektor DPS Administrator Danych podejmuje następujące kroki:

1. zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości i ciągłości pracy,
2. odbiera dokładną relację z zaistniałego naruszenia bezpieczeństwa Danych od osoby powiadamiając, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem, nawiązuje kontakt ze specjalistami zewnętrznymi (jeżeli zachodzi taka potrzeba, w szczególności w zakresie bezpieczeństwa informatycznego).

3. niezwłocznie powiadamia o sytuacji IODO, z którym konsultuje dalsze postępowanie.

§7

Administrator Danych (bądź IODO) dokumentuje zaistniały przypadek naruszenia bezpieczeństwa Danych sporządzając raport - Załącznik nr 1.

§8

Administrator Danych (bądź IODO) zasięga potrzebnych mu opinii i proponuje działania naprawcze (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia Danych z zabezpieczeń oraz terminu wznowienia przetwarzania Danych osobowych) - Załącznik nr 2 - rejestr incydentów i działań korygujących i zapobiegawczych

III. NARUSZENIE DANYCH OSOBOWYCH - ODPOWIEDZIALNOŚĆ

§9

Wobec osoby, która w przypadku naruszenia Danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się 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 aktualnie obowiązującym przepisami oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

IV. ZGŁASZANIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH ORGANOWI NADZORCZEMU

§10

1. W przypadku Naruszenia ochrony Danych osobowych, Dyrektor DPS bez zbędnej zwłoki – w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je Urzędowi ochrony danych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
2. Wzór zgłoszenia - Załącznik nr 3.
3. Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:
    a. opisywać 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;

b. zawierać imię nazwisko oraz Dane kontaktowe inspektora ochrony Danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;

c. opisywać możliwe konsekwencje Naruszenia ochrony Danych osobowych;

d. opisywać środki zastosowane lub proponowane przez Administratora w celu zapobiegania naruszeniu ochrony Danych osobowych, w tym w stosownych przypadkach – środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

1. Jeżeli – i w zakresie w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.
2. Administrator dokumentuje wszelkie naruszenia ochrony Danych osobowych, w tym okoliczności naruszenia ochrony Danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.

V. ZAWIADAMIANIE OSOBY, KTÓREJ DANE DOTYCZĄ, O NARUSZENIU OCHRONY DANYCH OSOBOWYCH

§11

1. Jeżeli Naruszenie ochrony Danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę której Dane dotyczą, o takim naruszeniu.
2. Zawiadomienie, o którym mowa w ust. 1 niniejszego artykułu, jasnym i prostym językiem opisuje charakter Naruszenia ochrony Danych osobowych oraz zawiera przynajmniej informacje i środki , o których mowa w § 10 ust. 2 lit. b), c) i d).
3. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:
   a. 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;
   b. Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której Dane dotyczą, o którym mowa w ust. 1;
   c. wymagałoby ono 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.

DYREKTOR
Domu Pomocy Społecznej "Zameczek"
w Kuźni Niedorowskiej
mgr Ewa Zamora

Załącznik 1

RAPORT Z NARUSZENIA OCHRONY DANYCH

1. Data ..... Godzina .....

2. Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane lub odpytane w związku z naruszeniem

   .....

   (imię, nazwisko, stanowisko służbowe,):

3. Lokalizacja zdarzenia .....

   (nr. pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.)

4. Rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu:

   .....

5. Podjęte działania:

   .....

6. Wstępna ocena przyczyn wystąpienia naruszenia:

   .....

7. Postępowanie wyjaśniające i naprawcze:

   .....

....

(podpis pracownika) (data i podpis Administratora/IODO)

Załącznik nr 2

REJESTR INCYDENTÓW BEZPIECZEŃSTWA ORAZ DZIAŁAŃ KORYGUJĄCYCH I ZAPOBIEGAWCZYCH

Zadanie / problem / incydent (*podać opis incydentu*)	Źródło zgłoszenia (*podać źródło zgłoszenia np. zawiadomienie, kontrola, itd.*)	Data rozpoczęcia	Data zakończenia	Odpowiedzialny za realizację (*podać Dane osoby lub funkcje osoby odpowiedzialnej*)	Przyczyna niezgodności (*podać przyczynę powstania incydentu*)	Działanie korygujące / zapobiegawcze (*opisać działania jakie podjęto w celu przywrócenia bezpieczeństwa*)	Ocena skuteczności (*opisać jakie skutki przyniosło działanie korygujące*)

Załącznik 3

Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu

W jaki sposób powiadomić Prezesa UODO o naruszeniu?
https://uodo.gov.pl/pl/134/233

Organem właściwym do zgłaszania naruszeń ochrony Danych osobowych jest Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO).

1. Zgłoszenia naruszenia dokonuje się elektronicznie **za pomocą odpowiedniego formularza dostępnego poniżej**, który należy wypełnić a następnie...
2. ...załączyć do **pisma ogólnego dostępnego** na platformie biznes.gov.pl