Zarządzenie nr 7/2019
Dyrektora Domu Pomocy Społecznej „SENIOR" im. Jana Kaczmarka w Czeladzi

z dnia 20 maja 2019 r.

w sprawie „Polityki bezpieczeństwa informacji" oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych" w Domu Pomocy Społecznej „SENIOR" im. Jana Kaczmarka w Czeladzi

Na podstawie art. 24 ust.1 Rozporządzenia Parlamentu Europejskiego i Rady 9UE) 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 (Dz.Urz. UE. L Nr 119, str. 1 z późn. zm.), oraz § 10 Regulaminu Organizacyjnego Domu Pomocy Społecznej „SENIOR" im. Jana Kaczmarka w Czeladzi przyjętego Zarządzeniem nr 270/2018 Burmistrza Miasta Czeladź z dnia 13 września 2018 r.

zarządzam co następuje:

§ 1. Wprowadzam w Domu Pomocy Społecznej „SENIOR" im. Jana Kaczmarka w Czeladzi „Politykę bezpieczeństwa informacji" stanowiącą załącznik nr 1 do niniejszego zarządzenia oraz „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych" stanowiącą załącznik nr 2 do niniejszego zarządzenia.

§ 2. Zobowiązuje się wszystkich pracowników przetwarzających w jakikolwiek sposób dane osobowe do stosowania zasad określonych w „Polityce bezpieczeństwa informacji" oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych" .

§ 3. Traci moc zarządzenie nr 12/2016 r. z dnia 10 listopada 2016 r. w sprawie „Polityki bezpieczeństwa przetwarzania danych osobowych" oraz 'Instrukcji zarządzania systemem informatycznym" w Domu Pomocy Społecznej „SENIOR" im. Jana Kaczmarka w Czeladzi.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
Domu Pomocy Społecznej
„SENIOR"
im. Jana Kaczmarka

mgr Dominik Hodurek

Załącznik nr 1
do Zarządzenia nr 7 /2019
Dyrektora Domu Pomocy
Społecznej„SENIOR”
im. Jana Kaczmarka w Czeladzi
z dnia 20 maja 2019 r.

Polityka Bezpieczeństwa Informacji w Domu Pomocy Społecznej „SENIOR” im. Jana Kaczmarka w Czeladzi

Podstawa prawna:

1.Rozporządzenie 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 przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO)
2.Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (tj. Dz. U. z 2018 r. poz. 1000 z póź.zm.).
3.Rozporządzenie Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych z dnia 29 kwietnia 2004 r. (Dz.U. Nr 100, poz. 1024)

§ 1. Celem Polityki Bezpieczeństwa danych osobowych, zwanej dalej Polityką Bezpieczeństwa, jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych w zakresie ochrony danych osobowych, sposobu przetwarzania w Domu Pomocy Społecznej „SENIOR” im. Jana Kaczmarka w Czeladzi.

§ 2. Określenia użyte w Polityce Bezpieczeństwa oznaczają:

1) jednostka – Dom Pomocy Społecznej „SENIOR” im. Jana Kaczmarka w Czeladzi;

2) dane osobowe – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, możliwa do zidentyfikowania osoba fizyczna to 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;

3) przetwarzanie – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

4) administrator - Dyrektor Domu Pomocy Społecznej „SENIOR” im. Jana Kaczmarka w Czeladzi;

5) administrator systemu – osoba upoważniona do zarządzania systemem informatycznym,

6) system informatyczny – system przetwarzania danych w Domu Pomocy Społecznej „SENIOR” im. Jana Kaczmarka w Czeladzi wraz z zasobami ludzkimi, technicznymi oraz finansowymi, który dostarcza i rozprowadza informacje;

7) zabezpieczenie systemu informatycznego – należy przez to rozumieć wdrożenie stosowanych środków administracyjnych, technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych a także ich utratą.

§ 3.1. Utrzymanie bezpieczeństwa przetwarzanych przez Jednostkę informacji rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności i dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z zasobem stanowiącym przedmiot niniejszej Polityki.

2. Dane osobowe muszą być:

1) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;

2) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;

3) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;

4) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane;

5) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane;

6) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych

§ 4.1. W systemie informacyjnym Jednostki przetwarzane są informacje służące do wykonywania zadań niezbędnych dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisów prawa.

2. Politykę Bezpieczeństwa stosuje się do:

1) danych osobowych mieszkańców domu przetwarzanych w formie papierowej oraz w systemie informatycznym,

2) wszystkich informacji dotyczących danych pracowników Jednostki, w tym danych osobowych personelu i treści zawieranych umów o pracę,

3) wszystkich danych kandydatów do pracy zbieranych na etapie rekrutacji,

4) informacji dotyczących zabezpieczenia danych osobowych,

5) rejestru osób dopuszczonych do przetwarzania danych osobowych,

6) innych dokumentów zawierających dane osobowe.

3. Zakresy określone przez dokumenty Polityki Bezpieczeństwa mają zastosowanie do całego systemu informacyjnego Jednostki w szczególności do:

1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są informacje podlegające ochronie,

2) wszystkich lokalizacji – pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,

3) wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, konsultantów, stażystów i innych osób mających dostęp do informacji podlegających ochronie.

4. Do stosowania zasad określonych przez dokumenty Polityki Bezpieczeństwa zobowiązani są wszyscy pracownicy w rozumieniu Kodeksu Pracy, konsultanci, stażyści oraz inne osoby mające dostęp do informacji podlegających ochronie.

§ 5.1. Wszystkie osoby, których rodzaj wykonywanej pracy będzie wiązał się z dostępem do danych osobowych, przed przystąpieniem do pracy, podlegają przeszkoleniu w zakresie obowiązujących przepisów prawa dotyczących ochrony danych osobowych oraz obowiązujących w Jednostce zasad ochrony danych osobowych.

2. Zakres czynności dla osoby dopuszczonej do przetwarzania danych osobowych powinien określać zakres odpowiedzialności tej osoby za ochronę danych osobowych w stopniu odpowiednim do zadań tej osoby realizowanych przy przetwarzaniu tych danych.

3. Udostępnianie danych osobowych podmiotom upoważnionym do ich otrzymania, na podstawie przepisów prawa, mogą być udostępnione jeżeli w sposób wiarygodny uzasadnią potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą.

4. Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.

§ 6. Dane osobowe udostępnia się na pisemny, umotywowany wniosek, który powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać zakres i przeznaczenie.

§ 7.1. Za bezpieczeństwo danych osobowych Jednostki, odpowiadają:

1) Administrator;

2) Inspektor Ochrony Danych Osobowych.

§ 8.1. Inspektor Ochrony Danych Osobowych:

1) sprawuje nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których dane są przetwarzane oraz kontrolą przebywających w nich osób,

2) identyfikuje i analizuje zagrożenia oraz ryzyko, na które narażone może być przetwarzanie danych osobowych w systemach informatycznych Jednostki,

3) sprawuje nadzór nad bezpieczeństwem danych zawartych w komputerach przenośnych, w których przetwarzane są dane osobowe,

4) sprawuje nadzór nad obiegiem oraz przechowywaniem dokumentów zawierających dane osobowe,

5) sprawuje nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane oraz kontrolą dostępu do danych,

6) powiadamia administratora systemu o konieczności zmianie/nadaniu uprawnień dostępu użytkownika do systemu,

7) prowadzi ewidencję osób zaangażowanych w przetwarzanie danych osobowych,

8) prowadzi rejestr zbiorów danych osobowych Jednostki (przetwarzanych metodą tradycyjną lub w systemach informatycznych).

§ 9.1. Administrator zobowiązany jest do przestrzegania wszystkich przepisów ustawy o ochronie danych, w szczególności poprzez:

1) określanie indywidualnych obowiązków i odpowiedzialności osób zatrudnionych przy przetwarzaniu danych osobowych, wynikających z ustawy o ochronie danych osobowych,

2) określenie pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego,

3) zapoznawanie osób zatrudnionych przy przetwarzaniu danych osobowych z przepisami obowiązującymi w tym zakresie,

4) wdrażanie i nadzorowanie przestrzegania Polityki bezpieczeństwa informacji,

5) stwarzanie warunków organizacyjnych i technicznych umożliwiających spełnienie wymogów wynikających z obowiązywania ustawy o ochronie danych osobowych,

6) odpowiedzialność za poprawność merytoryczną danych gromadzonych w systemach informacyjnych,

7) określanie, które osoby i na jakich prawach mają dostęp do danych informacji.

§ 10.1. Administrator Systemu Informatycznego odpowiedzialny jest za:

1) bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych,

2) optymalizację wydajności systemu informatycznego, baz danych,

3) instalacje i konfiguracje sprzętu sieciowego i serwerowego,

4) instalacje i konfiguracje oprogramowania systemowego, sieciowego, oprogramowania bazodanowego,

5) konfigurację i administrację oprogramowaniem systemowym, sieciowym oraz bazodanowym zabezpieczającym dane chronione przed nieupoważnionym dostępem,

6) współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych,

7) zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego,

8) zarządzanie kopiami awaryjnymi danych w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie,

9) przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,

10) przyznawanie na wniosek Administratora Danych, za zgodą Administratora Bezpieczeństwa Informacji ściśle określonych praw dostępu do informacji w danym systemie,

11) wnioskowanie do Administratora Bezpieczeństwa Informacji w sprawie procedur bezpieczeństwa i standardów zabezpieczeń,

12) zarządzanie licencjami, procedurami ich dotyczącymi,

13) prowadzenie profilaktyki antywirusowej.

2. Praca Administratora Systemu Informatycznego jest nadzorowana pod względem bezpieczeństwa przez Administratora Bezpieczeństwa Informacji.

§ 11.1. Przetwarzanie danych osobowych następuje w wyznaczonych pomieszczeniach zamykanych na klucz przez wyznaczone do tego celu osoby.

2. Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.

3. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia należy niszczyć w stopniu uniemożliwiającym ich odczytanie.

4. Urządzenia, dyski lub inne informatyczne nośniki danych, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

§ 12.1. W jednostce rozróżnia się następujące kategorie środków zabezpieczeń danych osobowych:

1) Zabezpieczenia fizyczne:

a) pomieszczenia zamykane na klucz,

b) szafy pancerne z zamkami,

2) Zabezpieczenia procesów przetwarzania danych w dokumentacji papierowej:

a) przetwarzanie danych osobowych następuje w wyznaczonych pomieszczeniach,

b) przetwarzanie danych osobowych następuje przez wyznaczone do tego celu osoby.

3) Zabezpieczenia organizacyjne:

a) osobą odpowiedzialną za bezpieczeństwo danych jest Administrator oraz Inspektor Ochrony Danych Osobowych,

b) ASI na bieżąco kontroluje pracę systemu informatycznego z należytą starannością, zgodnie z aktualnie obowiązującą w tym zakresie wiedzą i z obowiązującymi procedurami.

§ 13.1. Ustala się następującą organizację pracy przy przetwarzaniu danych osobowych i zasady przetwarzania:

1) w trakcie przetwarzania danych osobowych, pracownik jest osobiście odpowiedzialny za bezpieczeństwo powierzonych mu danych,

2) przed przystąpieniem do realizacji zadań związanych z przetwarzaniem danych osobowych, pracownik winien sprawdzić, czy posiadane przez niego dane były należycie zabezpieczone, oraz czy zabezpieczenia te nie były naruszone,

3) w trakcie przetwarzania danych osobowych, pracownik winien dbać o należyte ich zabezpieczenie przed możliwością wglądu, bądź zmiany przez osoby do tego celu nieupoważnione,

4) po zakończeniu przetwarzania danych pracownik winien należycie zabezpieczyć dane osobowe przed możliwością dostępu do nich osób nieupoważnionych.

§ 14.1. Za naruszenie ochrony danych osobowych uznaje się przypadki, gdy:

1) stwierdzono naruszenie zabezpieczenia systemu informatycznego lub naruszenie zabezpieczenia zbioru danych osobowych zebranych i przetwarzanych w innej formie,

2) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych.

§ 15. Każdy pracownik jednostki, który stwierdzi lub podejrzewa naruszenie ochrony danych osobowych w systemie informatycznym, lub przetwarzanych w inny sposób, zobowiązany jest do niezwłocznego poinformowania o tym administratora tego systemu informatycznego lub w przypadku jego nieobecności Inspektora Ochrony Danych Osobowych.

§ 16.1. Dane osobowe zostają ujawnione, gdy stają się znane w całości lub części pozwalającej na określenie osobom nieuprawnionym tożsamości osoby, której dane dotyczą.

2. W stosunku do danych, które zostały zagubione, pozostawione bez nadzoru poza obszarem bezpieczeństwa należy przeprowadzić postępowanie wyjaśniające, czy dane osobowe należy uznać za ujawnione.

§ 17.1. Gdy Administrator stwierdzi lub uzyska informację wskazującą na naruszenie ochrony tej bazy danych zobowiązany jest do niezwłocznego:

1) zapisania wszelkich informacji i okoliczności związanych z danym zdarzeniem, a w szczególności dokładnego czasu uzyskania informacji o naruszeniu ochrony danych osobowych lub samodzielnym wykryciu tego faktu,

2) jeżeli zasoby systemu na to pozwalają, wygenerowania i wydrukowania wszystkich dokumentów i raportów, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzenia ich datą i podpisania,

3) przystąpienia do zidentyfikowania rodzaju zaistniałego zdarzenia, w tym do określenia skali zniszczeń, metody dostępu osoby niepowołanej do danych itp.,

4) podjęcia odpowiednich kroków w celu powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia ochrony danych, w tym m.in.:

a) szczegółowej analizy stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych,

b) przywrócenia normalnego działania systemu, przy czym, jeżeli nastąpiło uszkodzenie bazy danych, odtworzenia jej z ostatniej kopii awaryjnej z zachowaniem wszelkich środków ostrożności mających na celu uniknięcie ponownego uzyskania dostępu przez osobę nieupoważnioną, tą samą drogą,

2. W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki - w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia - zgłasza je Prezesowi Urzędu Ochrony Danych Osobowych.

3. Po przywróceniu normalnego stanu bazy danych osobowych należy przeprowadzić szczegółową analizę w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia, oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości. Jeżeli przyczyną zdarzenia był błąd użytkownika systemu informatycznego, należy przeprowadzić szkolenie wszystkich osób biorących udział w przetwarzaniu danych.

4. Jeżeli przyczyną zdarzenia była infekcja wirusem należy ustalić źródło jego pochodzenia i wykonać zabezpieczenia antywirusowe i organizacyjne wykluczające powtórzenie się podobnego zdarzenia w przyszłości.

5. Jeżeli przyczyną zdarzenia było zaniedbanie ze strony użytkownika systemu należy wyciągnąć konsekwencje.

§ 18.1. Każda jednostka realizująca na rzecz DPS umowę, musi zostać zobowiązana do zachowania poufności informacji uzyskanych w trakcie realizacji poprzez odpowiednie zapisy umowy. Wzór umowy powierzenia przetwarzania danych osobowych stanowi **załącznik nr 1.**
Dodatkowo, każdy z pracowników/podwykonawców strony umowy realizujący czynności w ramach tej umowy, musi zostać zobowiązany do imiennego oświadczenia o zachowaniu poufności. Wzór oświadczenia określa **załącznik nr 2**.

2. Każda osoba dopuszczona do przetwarzania danych osobowych musi otrzymać pisemne upoważnienie od ADO do przetwarzania tych danych. Wzór upoważnienia do przetwarzania danych osobowych stanowi **załącznik nr 3**.

3. Osoby przebywające w obszarach przetwarzania danych osobowych w związku z wykonywaniem czynności w ramach umowy zawartej z DPS, a nie dopuszczone do przetwarzania danych osobowych są zobowiązane jedynie do imiennego oświadczenia o zachowaniu poufności, o którym mowa w punkcie 1.

4. Do przetwarzania danych osobowych mogą zostać dopuszczone tylko i wyłącznie osoby, które otrzymały pisemne upoważnienie od ADO lub uprawnionej przez niego osoby (IOD).

5. Za nadawanie upoważnień odpowiedzialny jest ADO lub osoby pisemnie do tego upoważnione (IOD). Upoważnienie do przetwarzania danych osobowych, jest nadawane przed przystąpieniem osoby do przetwarzania danych oraz po zapoznaniu się przez nią z przepisami w zakresie ochrony danych osobowych. Upoważnienie jest nadawane w zakresie i na czas zgodny z powierzonymi obowiązkami. Osoba upoważniona przyjmuje i potwierdza zobowiązanie do poufności, składając czytelny podpis pod treścią oświadczenia na otrzymanym upoważnieniu. Oryginały upoważnień przechowywane są w komórce DPS odpowiedzialnej za ich przygotowanie, a kopia zostaje przekazana osobie upoważnionej.

6. Za zmianę upoważnień odpowiedzialny jest ADO. Upoważnienie jest zmieniane niezwłocznie po zmianie zakresu obowiązków osoby upoważnionej, w zakresie zgodnym ze zmianą, która nastąpiła. Zmiana upoważnienia dokonywana poprzez wystąpienie z wnioskiem bezpośredniego przełożonego pracownika lub kierownika jego komórki organizacyjnej, o odwołanie aktualnego upoważnienia do przetwarzania danych osobowych.

7. Za odwołanie upoważnień odpowiedzialny jest ADO. Upoważnienie jest odwoływanie niezwłocznie po ustąpieniu współpracy z osobą upoważnioną lub zmianą jej obowiązków, w zakresie takim, że dalsze przetwarzanie danych nie będzie miało miejsca.

8. Rejestr upoważnień ma na celu kontrolę nad tym kto i kiedy otrzymał upoważnienie do przetwarzania danych osobowych, czy to upoważnienie jest ważne oraz czy jego zakres jest aktualny. Rejestr prowadzony jest w formie papierowej i odzwierciedla aktualny stan.

9. Każde nadanie lub odwołanie upoważnienia jest odnotowywane w rejestrze upoważnień przez wyznaczonego pracownika komórki DPS odpowiedzialnej za jego prowadzenie. Strukturę danych rejestru upoważnień stanowi **załącznik nr 4**. W rejestrze odnotowuje się informacje o imieniu i nazwisku,

osoby której nadanie lub odwołanie upoważnienia dotyczy, stanowisku, dacie nadania upoważnienia i jego ustania, zakresie upoważnienia oraz nadanych identyfikatorach do systemu informatycznego.

§ 19.1. Zgoda osoby, której dane dotyczą jest zawsze potrzebna, jeżeli nie istnieje żadna inna przesłanka legalności przetwarzania określona w art. 6 RODO.

2. Wzór zgody na przetwarzanie danych osobowych stanowi **załącznik nr 5**.

3. W przypadku zbierania danych osobowych od osoby, której one dotyczą, o ile przepisy szczególne nie stanowią inaczej, DPS - ADO jest zobowiązany poinformować tę osobę o:

1) swojej tożsamości i danych kontaktowych oraz, gdy ma to zastosowanie wskazać tożsamość i dane kontaktowe swojego przedstawiciela;

2) gdy ma to zastosowanie - dane kontaktowe inspektora ochrony danych;

3) cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania;

4) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f RODO - prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;

5) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;

6) gdy ma to zastosowanie - informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej;

7) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;

8) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;

9) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a RODO) - informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;

10) informacje o prawie wniesienia skargi do organu nadzorczego;

11) informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;

4. Wzór klauzuli informacyjnej dla osoby od której zbierane są dane, stanowi **załącznik nr 6**.

5. W przypadku zbierania danych osobowych nie od osoby, której dane dotyczą, o ile przepisy szczególne nie stanowią inaczej DPS-ADO jest zobowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych wskazując:

1) swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;

2) gdy ma to zastosowanie - dane kontaktowe inspektora ochrony danych;

3) cele przetwarzania, do których mają posłużyć dane osobowe, oraz podstawę prawną przetwarzania;

4) kategorie odnośnych danych osobowych;

5) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;

6) gdy ma to zastosowanie - informacje o zamiarze przekazania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej,

7) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;

8) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) RODO - prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;

9) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;

10) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a RODO) - informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;

11) informacje o prawie wniesienia skargi do organu nadzorczego;

12) źródło pochodzenia danych osobowych, a gdy ma to zastosowanie - czy pochodzą one ze źródeł publicznie dostępnych;

6. Wzór klauzuli informacyjnej, dla osoby, której dane pozyskano z innego źródła, niż ona sama, stanowi **załącznik nr 7**.

§ 20.1. Ochrona wizerunku mieszkańców - ochrona danych biometrycznych – zdjęć, fotografii, przysługuje na podstawie RODO oraz ustawy o prawie autorskim i prawach pokrewnych. Rozpowszechnianie wizerunku osoby wymaga jej zgody oraz podania sposobu jego rozpowszechniania.

§ 21.1. Wykaz budynków, pomieszczeń lub części pomieszczeń stanowiących obszar przetwarzania danych osobowych stanowi **załącznik nr 8.**

2. Analiza ryzyka i zagrożeń w DPS stanowi **załącznik nr 9.**

Załącznik nr 1
do Polityki Bezpieczeństwa Informacji
w Domu Pomocy Społecznej „SENIOR”
im. Jana Kaczmarka w Czeladzi

Umowa powierzenia przetwarzania danych osobowych

zawarta w dniu …….. r. w Czeladzi w związku z trwającą umową nr ……..z dnia …… r. pomiędzy:
Miasto Czeladź - Dom Pomocy Społecznej „SENIOR” im Jana Kaczmarka z siedzibą w Czeladzi przy ul. Szpitalnej 5A, reprezentowany przez:
Dyrektora – ……..…… – zwanym w dalszej części umowy **„Administratorem”**
oraz
……, zwanym w dalszej części umowy **„Podmiotem przetwarzającym”**

Preambuła

W związku z realizacją umowy nr …….. z dn. ….. r. zawartej pomiędzy Administratorem a Podmiotem przetwarzającym, której przedmiotem jest sprawowanie bieżącego nadzoru z zakresu …… (zwana dalej "Umową główną") strony niniejszej umowy mając w szczególności na uwadze ochronę praw i wolności osób fizycznych w zakresie prawa do ochrony danych osobowych, uwzględniając postanowienia 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) postanawiają, co następuje:

§ 1

Powierzenie przetwarzania danych osobowych

1. W trybie art. 28 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) – zwanego w dalszej części „RODO” - Administrator powierza Podmiotowi przetwarzającemu dane osobowe do przetwarzania w celu realizacji postanowień określonych w umowie głównej, na zasadach określonych w niniejszej umowie.
2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, RODO oraz innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi RODO.

§2

Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał, powierzone na podstawie umowy dane zwykłe …… ….. .
2. Powierzone przez Administratora dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu realizacji umowy głównej.

§3

Obowiązki podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanemu z przetwarzaniem danych osobowych, o których mowa w art. 32 RODO.
2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy.
4. Podmiot przetwarzający zobowiązuje się przekazać Administratorowi imienny wykaz osób

upoważnionych, które będą przetwarzać dane osobowe zgodnie z postanowieniami niniejszej umowy, wg wzoru określonego w załączniku do umowy.
5. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, o której mowa w art. 28 ust. 3 pkt b RODO przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
6. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem, zależnie od decyzji Administratora: trwale usuwa lub zwraca Administratorowi wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii Europejskiej lub prawo jej państwa członkowskiego nakazują temu podmiotowi przechowywanie danych osobowych. W przypadku, gdy na Podmiocie przetwarzającym ciąży obowiązek przechowywania danych osobowych niezwłocznie po zakończeniu obowiązywania umowy składa on Administratorowi stosowne oświadczenie w tym zakresie ze wskazaniem podstawy prawnej tego obowiązku. Jeśli Administrator w trakcie trwania umowy nie przedstawi na piśmie swojej decyzji co do usunięcia lub zwrotu danych przyjmuje się, iż oczekuje on ich usunięcia.
7. W przypadku, gdy zgodnie z ust. 6, podmiot przetwarzający usuwa dane przechowywane na elektronicznych nośnikach danych, zarówno w ramach systemów informatycznych jak i na nośnikach zamontowanych w urządzeniach elektronicznych usunięcie to dokonywane jest w sposób, który nie pozwala na odzyskanie danych przy wykorzystaniu aktualnie dostępnych środków technicznych.
8. W przypadku, gdy w trakcie realizacji świadczenia opisanego w umowie głównej zachodzi konieczność przeniesienia urządzeń elektronicznych posiadających nośniki zawierające dane osobowe poza obszar budynków zarządzanych przez Administratora podmiot przetwarzający demontuje te nośniki i protokolarnie przekazuje Administratorowi. W przypadku, gdy demontaż nośnika jest niemożliwy lub wiązałby się ze zbytnią ingerencją w strukturę urządzenia Podmiot przetwarzający zapewnia ochronę zawartych na nich danych osobowych zgodnie z postanowieniami niniejszej umowy i powszechnie obowiązujących przepisów prawa.
9. Na okoliczność opisanych w ust. 6 i 7:
a) usunięcia danych – Podmiot przetwarzający niezwłocznie składa Administratorowi stosowne oświadczenie o usunięciu danych,
b) zwrocie danych – Podmiot przetwarzający i Administrator niezwłocznie sporządzają stosowny protokół o zwrocie danych.
10. W miarę możliwości Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą w zakresie wykonywania jej praw określonych w rozdziale III RODO oraz wywiązywania się z obowiązków określonych w art. 32-36 RODO.
11. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je Administratorowi danych, jednakże nie później niż w ciągu 12 godzin od jego stwierdzenia.
12. Zgłoszenie, o którym mowa w ust. 11 musi zostać przekazane do ……. w siedzibie Administratora w formie pisemnej, zawierającej co najmniej:
a) opis charakteru 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) opis możliwych konsekwencji naruszenia ochrony danych osobowych,
c) opis środków zastosowanych lub proponowanych przez Podmiot przetwarzający w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków,
d) zawierać imię i nazwisko oraz dane kontaktowe pracownika Podmiotu przetwarzającego, od którego można uzyskać więcej informacji,
e) w przypadku niedochowania terminu, o którym mowa w ust. 11, określenie jego przyczyny.

§4

Prawo kontroli

1. Administrator zgodnie z art. 28 ust. 3 pkt h) RODO ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.
2. Administrator realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum 3 dniowym jego uprzedzeniem.
3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych nie dłuższym niż 7 dni.
4. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO.

§5

Dalsze powierzenie danych do przetwarzania

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania innemu podmiotowi jedynie w celu wykonania umowy głównej po uzyskaniu uprzedniej pisemnej zgody Administratora.
2. Przekazanie powierzonych danych do państwa trzeciego lub organizacji międzynarodowej może nastąpić jedynie na pisemne polecenie Administratora chyba, że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii Europejskiej lub prawo jej państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje pisemnie Administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Na inny podmiot, o którym mowa w ust. 1 nałożone zastają obowiązki jakie zostały nałożone na Podmiot przetwarzający w niniejszej umowie.
4. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązanie się ze spoczywających na innym podmiocie, o którym mowa w ust. 1, obowiązków ochrony danych.

§ 6

Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez organ nadzorczy, o którym mowa w art. 51 RODO. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora.

§7

Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej.
2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych, o których mowa w ust. 1, nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora danych w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa.

§8

Czas obowiązywania umowy

1. Niniejsza umowa obowiązuje od dnia zawarcia do zakończenia obowiązywania umowy głównej.
2. Naruszenie zasad przetwarzania danych wynikających z umowy stanowi podstawę do rozwiązania umowy głównej ze skutkiem natychmiastowym z przyczyn, za które odpowiedzialność ponosi Podmiot przetwarzający.

§9

Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.
2. W sprawach nieuregulowanych niniejszą umową zastosowanie będą miały przepisy RODO oraz innych przepisów prawa powszechnie obowiązującego.
3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy dla Administratora.

…..... ……...

Administrator **Podmiot przetwarzający**

Załącznik nr 1
do umowy powierzenia
przetwarzania danych osobowych

Imienny wykaz osób upoważnionych

Zgodnie z §3 ust. 4 umowy powierzenia przetwarzania danych osobowych zawartej w dn…….r. w związku z trwającą umową nr …….. z dn. …….. r. oświadczam, że osobami upoważnionymi, które będą przetwarzać dane osobowe zgodnie z postanowieniami umowy są:

L.P.	Imię i Nazwisko	Stanowisko
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

…….....……...
(podpis osoby reprezentującej Podmiot przetwarzający)

Załącznik nr 2
do Polityki Bezpieczeństwa Informacji
w Domu Pomocy Społecznej „SENIOR”
im. Jana Kaczmarka w Czeladzi

Oświadczenie o zachowaniu poufności informacji

uzyskanych w związku z realizacją umowy

Ja niżej podpisany …… ……....,

będąc pracownikiem Wykonawcy / Podwykonawcą / pracownikiem podwykonawcy* zobowiązuję się do nieograniczonego w czasie zachowania w tajemnicy wszelkich informacji uzyskanych w związku z realizacją umowy …… niezależnie od formy przekazania tych informacji oraz ich źródła, a w szczególności informacji dotyczących spraw prowadzonych przez DPS ‘SENIOR” im. Jana Kaczmarka w Czeladzi, a także informacji technologicznych, technicznych, organizacyjnych i innych informacji, których ujawnienie mogłoby spowodować szkodę dla prawnie chronionych interesów DPS ‘SENIOR” im. Jana Kaczmarka w Czeladzi.

…….

/podpis/

Załącznik nr 3
do Polityki Bezpieczeństwa Informacji
w Domu Pomocy Społecznej „SENIOR”
im. Jana Kaczmarka w Czeladzi

Upoważnienie do przetwarzania danych osobowych

Administrator danych osobowych: …… **– Dyrektor Domu Pomocy Społecznej „SENIOR” im. Jana Kaczmarka w Czeladzi dnia ……r.** nadaje upoważnienie dla Pana/Pani : **……**
Stanowisko służbowe: **……**

Upoważniony otrzymuje dostęp do poniższych zasobów danych osobowych w celu ich przetwarzania: (w formie tradycyjnej/w systemie informatycznym)

W zakresie: **bez ograniczeń/podglądu danych/wprowadzania danych/ zmieniania danych**
Upoważnienie nadaje się do ustania stosunku pracy. Wszelakie poprzednie upoważnienia do przetwarzania danych osobowych z dniem wprowadzenia niniejszego wygasają. Jednocześnie bieżące upoważnienie zostaje zawieszone w przypadku długiej nieobecności / urlopu. Po upływie w/w okresu nieobecności / urlopu upoważniony(a) wykonując obowiązki wynikające z upoważnienia otrzymuje ponowne upoważnienie niniejszym dokumentem.
Na podstawie niniejszego upoważnienia

OŚWIADCZENIE UPOWAŻNIONEGO

Ja niżej podpisany/a, oświadczam, że zostałem/am zaznajomiony/a z przepisami dotyczącymi ochrony danych osobowych, w tym z Rozporządzeniem 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 przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO) oraz ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (tj. Dz. U. z 2018 r. poz. 1000). Ponadto zapoznałem/am się z zasadami dotyczącymi ochrony danych osobowych obowiązujących w Domu Pomocy Społecznej „SENIOR” im. Jana Kaczmarka w Czeladzi w tym m.in. zapisanymi w Polityce bezpieczeństwa informacji oraz w Instrukcji zarządzania systemem informatycznym i zobowiązuję się do ich przestrzegania.

Jednocześnie oświadczam że :
1. Zobowiązuję się do zachowanie w tajemnicy danych osobowych, do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań służbowych i obowiązków pracowniczych, zarówno w trakcie wiążącego mnie stosunku pracy, jak i po ustaniu zatrudnienia.
2. Zapewnię ochronę danym przetwarzanym, a w szczególności zabezpieczę je przed dostępem osób nieupoważnionych, zabraniem, uszkodzeniem oraz nieuzasadnioną modyfikacją lub zniszczeniem.
3. Natychmiast zgłoszę stwierdzenie próby lub faktu naruszenia zasad ochrony danych osobowych lub bezpieczeństwa systemy informatycznego, w którym przetwarzane są dane osobowe.
4. Przyjmuję do wiążącej wiadomości, iż postępowanie rażąco sprzeczne z wyżej wskazanymi obowiązkami i przepisami prawa, może być uznane za ciężkie naruszenie obowiązków pracowniczych.

Podpisy:

…… ……...
Administrator danych osobowych Osoba upoważniona

Załącznik nr 4
do Polityki Bezpieczeństwa Informacji
w Domu Pomocy Społecznej „SENIOR”
im. Jana Kaczmarka w Czeladzi

Rejestr osób upoważnionych do przetwarzania danych osobowych w DPS „SENIOR”

Lp.	Imię i nazwisko	Stanowisko służbowe	Data nadania upoważnienia	Data ustania upoważnienia	Wykaz zbiorów danych wynikających z upoważnienia	Identyfikator *(Jeżeli dane są przetwarzane w systemie informatycznym)*

Data i podpis Administratora Danych Osobowych

…….....

Załącznik nr 5
do Polityki Bezpieczeństwa Informacji
w Domu Pomocy Społecznej „SENIOR”
im. Jana Kaczmarka w Czeladzi

……

Imię i nazwisko

Klauzula wyrażenia zgody na przetwarzanie danych osobowych przez osobę, której dane dotyczą:

1. Wyrażam zgodę/nie wyrażam zgody* na przetwarzanie przez Dom Pomocy Społecznej „SENIOR” im. Jana Kaczmarka w Czeladzi z siedzibą w Czeladzi przy ul. Szpitalnej 5A, nr tel. sekretariat: 32/265-94-00, email: senior@seniorczeladz.com moich danych osobowych w celu i na czas niezbędny do realizacji zadań Domu Pomocy Społecznej wynikających z przepisów ustawy z dnia 12 marca 2004 r. o pomocy społecznej oraz wydane na jej podstawie przepisy wykonawcze (w tym rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 23 sierpnia 2012 r. w sprawie domów pomocy społecznej), ustawy z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych oraz wydane na jej podstawie przepisy wykonawcze, Statutu oraz Regulaminu Organizacyjnego oraz innych przepisów prawa, które regulują działanie DPS. Dane będą przechowywane przez okres wymagany przez przepisy.

……

podpis

2. Wyrażam zgodę/nie wyrażam zgody* na przetwarzanie oraz wykorzystanie przez Dom Pomocy Społecznej „SENIOR” im. Jana Kaczmarka w Czeladzi z siedzibą w Czeladzi przy ul. Szpitalnej 5A, mojego wizerunku, utrwalonego na fotografiach lub filmach wykorzystywanych w celach promocyjnych, archiwizacyjnych oraz digitalizacyjnych. Mój wizerunek może zostać w szczególności wykorzystany na stronie internetowej, profilach zarządzanych przez Dom Pomocy Społecznej „SENIOR” oraz mediach. Zgoda udzielona jest na okres działalności Administratora.

……

podpis

3. Wyrażam zgodę/nie wyrażam zgody* na przetwarzanie przez Dom Pomocy Społecznej „SENIOR” im. Jana Kaczmarka w Czeladzi z siedzibą w Czeladzi przy ul. Szpitalnej 5A, nr tel. sekretariat: 32/265-94-00, email: senior@seniorczeladz.com moich danych osobowych wskazanych poniżej w celu kontaktowania się Administratora przez okres trwania stosunku pracy ze skutkiem na koniec roku, w formie kontaktu:
   1) telefonicznego: pod nr telefonu:
      ……..……..
   2) mailowego: pod adresem:
      ……..…….
   3) za pomocą korespondencji pocztowej:
      ……..……..

……

podpis

Wyrażenie woli zgodne jest z postanowieniami 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.
Potwierdzam otrzymanie załącznika informacyjnego zgodnie z art. 13 ust. 1 i ust. 2 ogólnego rozporządzenia o ochronie danych osobowych UE 2016/679 z dnia 27 kwietnia 2016 r. od Administratora Danych Osobowych Domu Pomocy Społecznej „SENIOR” im. Jana Kaczmarka, z siedzibą przy ul. Szpitalnej 5A, 41-250 Czeladź, z którym się zapoznałem i przyjąłem do wiadomości.

……

podpis* - niepotrzebne skreślić

Załącznik nr 1

Załącznik informacyjny w związku z wyrażeniem zgody

W związku z wyrażeniem przez Pana/Panią zgody na przetwarzanie danych osobowych, spełniając prawny obowiązek zgodnie z art. 13 ust. 1 i ust. 2 ogólnego rozporządzenia o ochronie danych osobowych UE 2016/679 z dnia 27 kwietnia 2016 r. informuję, że:

1) Administratorem Danych Osobowych jest Dom Pomocy Społecznej „SENIOR" im. Jana Kaczmarka z siedzibą w Czeladzi przy ul. Szpitalnej 5A reprezentowanym przez Dyrektora – Dominika Hodurek,

2) Inspektorem Ochrony Danych Osobowych w Domu Pomocy Społecznej „SENIOR" im. Jana Kaczmarka z siedzibą w Czeladzi przy ul. Szpitalnej 5A jest Agnieszka Wiejak, e-mail: wiejak.agnieszka098@gmail.com

3) Celem przetwarzania danych osobowych jest zatrudnienie i wykonanie wobec pracowników czynności z zakresu prawa pracy, prowadzenia polityki kadrowo-płacowej oraz kontaktowania się w sprawach pracowniczych na podstawie art. 6 ust. 1 pkt. a oraz b;

4) Podstawą prawną przetwarzania danych jest:

   a) Wypełnienie obowiązku wynikającego z przepisów prawa – art. 6 ust. 1 lit. c RODO, ustawa z dnia 26.06.1974 r. – Kodeks pracy (tekst jedn. Dz.U. z 2018 poz. 917 z późn. zm.)

   b) Realizacja celów wynikających z uzasadnionych interesów realizowanych przez Administratora.

5) Na podstawie obowiązujących przepisów prawa, jeśli będzie to konieczne, Pana/Pani dane będą udostępniane innym administratorom, a także podmiotom przetwarzającym oraz osobom upoważnionym do przetwarzania danych osobowych, które musza mieć dostęp aby wykonywać swoje obowiązki. Wymienieni odbiorcy zostaną zobowiązani do zachowania danych osobowych w poufności w procesie ich przechowywania.

6) Pani/Pana dane osobowe będą przetwarzane przez okres wymagany przez przepisy prawa w przypadku danych związanych ze stosunkiem pracy.

7) posiada Pani/Pan prawo dostępu do wszystkich przekazanych i przetwarzanych danych osobowych oraz prawo ich sprostowania, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, które wyrażono na podstawie zgody przed jej cofnięciem;

8) ma Pan/Pani prawo wniesienia skargi do organu nadzorczego, gdy poweźmie informację lub uzna Pan/Pani, że przetwarzanie powierzonych danych osobowych narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.

9) Dane osobowe, którymi zarządza Administrator nie będą przekazywane do odbiorców w państwach trzecich, tj. poza Europejski Obszar Gospodarczy (EOG) lub do organizacji międzynarodowych.

10) Dane osobowe zbierane przez Administratora nie będą wykorzystywane w procesach zautomatyzowanego podejmowania decyzji lub do profilowania.

Załącznik nr 6
do Polityki Bezpieczeństwa Informacji
w Domu Pomocy Społecznej „SENIOR”
im. Jana Kaczmarka w Czeladzi

Załącznik informacyjny w związku z wyrażeniem zgody

Na podstawie art. 13 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 (RODO) Dom Pomocy Społecznej „SENIOR” im. Jana Kaczmarka w Czeladzi przekazuje następujące informacje związane z przetwarzaniem danych osobowych:

DANE ADMINISTRATORA

Dom Pomocy Społecznej „SENIOR” im. Jana Kaczmarka w Czeladzi z siedzibą w Czeladzi przy ul. Szpitalnej 5A, nr tel. sekretariat: 32/265-94-00, email: senior@seniorczeladz.com

INSPEKTOR OCHRONY DANYCH

Administrator wyznaczył Inspektora Ochrony Danych (IOD), z którym kontakt jest możliwy pod adresem: wiejak.agnieszka098@gmail.com

CEL I SPOSÓB PRZETWARZANIA DANYCH

Przetwarzanie danych u Administratora następuje w celu realizacji zadań DPS wynikających z przepisów:

1. ustawa z dnia 12 marca 2004 r. o pomocy społecznej oraz wydane na jej podstawie przepisy wykonawcze (w tym rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 23 sierpnia 2012 r. w sprawie domów pomocy społecznej),
2. ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych oraz wydane na jej podstawie przepisy wykonawcze,
3. Statutu oraz Regulaminu Organizacyjnego
4. innych przepisów prawa, które regulują działanie DPS.

Wszelkie dane osobowe pozyskane przez Administratora przetwarzane są w postaci papierowej lub elektronicznej. Administrator zapewnia właściwe zabezpieczenie techniczne i informatyczne pozyskanych danych.

PODSTAWA PRAWNA PRZETWARZANIA DANYCH OSOBOWYCH

1. Przetwarzanie danych mieszkańców następuje na podstawie decyzji kierującej wystawionej przez Ośrodek Pomocy Społecznej lub wyrażonej zgody.
2. W przypadku mieszkańców DPS oraz ich opiekunów prawnych/kuratorów obowiązek podania danych osobowych wynika z przepisów prawa.

UDOSTĘPNIANIE DANYCH OSOBOWYCH

Dane osobowe pozyskane przez Administratora mogą być udostępniane:

1. pracownikom DPS na podstawie upoważnień do przetwarzania danych celem realizacji obowiązków służbowych,
2. podmiotom zewnętrznym zajmującym się bieżącą obsługą DPS,
3. organom władzy publicznej oraz podmiotom wykonującym zadania publiczne lub działającym na zlecenie organów władzy publicznej, w zakresie i w celach, które wynikają z przepisów prawa.

OKRES, PRZEZ KTÓRY ADMINISTRATOR PRZETWARZA DANE

Dane osobowe pozyskane przez Administratora będą przechowywane przez okres niezbędny dla realizacji prawnie uzasadnionych obowiązków, a także interesów Administratora, w tym do prawidłowego wykonania decyzji kierujących mieszkańców do DPS oraz umów zawieranych przez Administratora. Dane będą przetwarzane przez okres wynikający również z przepisów ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (tj. Dz. U. z 2018 r. poz. 217 z późn. zm.)

PRZEKAZYWANIE DANYCH OSOBOWYCH DO PAŃSTWA TRZECIEGO

Dane osobowe, którymi zarządza Administrator nie będą przekazywane do odbiorców w państwach trzecich, tj. poza Europejski Obszar Gospodarczy (EOG) lub do organizacji międzynarodowych.

UPRAWNIENIA OSOBY, KTÓREJ DANE DOTYCZĄ

W związku z przetwarzaniem danych osobowych, osobie której dane dotyczą przysługuje prawo do:

1) dostępu do danych osobowych, w tym prawo do uzyskania kopii tych danych;
2) żądania sprostowania (poprawiania) danych osobowych – w przypadku gdy dane są nieprawidłowe lub niekompletne;
3) żądania usunięcia danych osobowych (tzw. „prawo do bycia zapominanym") – w przypadku gdy:

a) dane nie są już niezbędne do celów, dla których były zebrane lub w inny sposób przetwarzane,
b) osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania danych,
c) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania,
d) dane przetwarzane są niezgodnie z prawem,
e) dane muszą być usunięte w celu wywiązania się z obowiązku wynikającego z przepisów prawa;

4) żądania ograniczenia przetwarzania danych osobowych – w przypadku gdy:

a) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych,
b) przetwarzanie danych jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych, żądając w zamian ich ograniczenia,
c) Administrator nie potrzebuje już danych dla swoich celów, ale osoba, której dane dotyczą, potrzebuje ich do ustalenia, obrony lub dochodzenia roszczeń,
d) osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania danych – do czasu ustalenia, czy prawnie uzasadnione podstawy po stronie Administratora są nadrzędne wobec podstawy sprzeciwu;

5) przenoszenia danych osobowych – w przypadku gdy:

a) przetwarzanie odbywa się na podstawie umowy zawartej z osobą, której dane dotyczą lub na podstawie zgody wyrażonej przez taką osobę oraz
b) przetwarzanie odbywa się w sposób zautomatyzowany;

6) sprzeciwu wobec przetwarzania danych osobowych, w tym profilowania, gdy zaistnieją przyczyny związane z Państwa szczególną sytuacją, a przetwarzanie danych oparte jest na podstawie niezbędności do celów wynikających z prawnie uzasadnionego interesu.

W przypadku przetwarzania danych na podstawie zgody osoby, której dane dotyczą, przysługuje prawo do cofnięcia zgody. Cofnięcie zgody nie ma wpływu na zgodność z prawem przetwarzania danych, którego dokonano na podstawie zgody przed jej wycofaniem.

Osobie, która uzna, że przetwarzanie jej danych osobowych narusza przepisy Rozporządzenia RODO przysługuje prawo wniesienia skargi do organu nadzorczego - **Prezes Urzędu Ochrony Danych Osobowych**

INFORMACJA O ZAUTOMATYZOWANYM SPOSOBIE PRZETWARZANIA DANYCH

Dane osobowe zbierane przez Administratora nie będą wykorzystywane w procesach zautomatyzowanego podejmowania decyzji lub do profilowania.

Załącznik nr 7
do Polityki Bezpieczeństwa Informacji
w Domu Pomocy Społecznej „SENIOR”
im. Jana Kaczmarka w Czeladzi

Wzór klauzuli informacyjnej, dla osoby, której dane pozyskano

- Administratorem danych osobowych jest Dom Pomocy Społecznej „SENIOR” im. Jana Kaczmarka w Czeladzi z siedzibą w Czeladzi przy ul. Szpitalnej 5A, nr tel. sekretariat: 32/265-94-00, email: senior@seniorczeladz.com
- Administrator wyznaczył Inspektora Ochrony Danych (IOD), z którym kontakt jest możliwy pod adresem: wiejak.agnieszka098@gmail.com
- Przetwarzanie danych u Administratora następuje w celu realizacji zadań DPS wynikających z przepisów: ustawa z dnia 12 marca 2004 r. o pomocy społecznej oraz wydane na jej podstawie przepisy wykonawcze (w tym rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 23 sierpnia 2012 r. w sprawie domów pomocy społecznej), Statutu oraz Regulaminu Organizacyjnego, innych przepisów prawa, które regulują działanie DPS i będą udostępniane jedynie podmiotom uprawnionym na podstawie przepisów prawa lub umów powierzenia.
- Wszelkie dane osobowe pozyskane przez Administratora przetwarzane są w postaci papierowej lub elektronicznej. Administrator zapewnia właściwe zabezpieczenie techniczne i informatyczne pozyskanych danych
- Dane osobowe pozyskane przez Administratora będą przechowywane przez okres niezbędny dla realizacji prawnie uzasadnionych obowiązków, a także interesów Administratora, w tym do prawidłowego wykonania decyzji kierujących mieszkańców do DPS oraz umów zawieranych przez Administratora. Dane będą przetwarzane przez okres wynikający również z przepisów ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (tj. Dz. U. z 2018 r. poz. 217 z późn. zm.)
- Dane osobowe, którymi zarządza Administrator nie będą przekazywane do odbiorców w państwach trzecich, tj. poza Europejski Obszar Gospodarczy (EOG) lub do organizacji międzynarodowych.
- Dane osobowe zbierane przez Administratora nie będą wykorzystywane w procesach zautomatyzowanego podejmowania decyzji lub do profilowania:
  - w związku z przetwarzaniem danych osobowych, osobie której dane dotyczą przysługuje prawo do:
  - dostępu do danych osobowych, w tym prawo do uzyskania kopii tych danych;
  - żądania sprostowania (poprawiania) danych osobowych – w przypadku gdy dane są nieprawidłowe lub niekompletne;
  - żądania usunięcia danych osobowych (tzw. „prawo do bycia zapominanym”) – w przypadku gdy:
  - dane nie są już niezbędne do celów, dla których były zebrane lub w inny sposób przetwarzane,
  - osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania danych,
  - osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania,
  - dane przetwarzane są niezgodnie z prawem,
  - dane muszą być usunięte w celu wywiązania się z obowiązku wynikającego z przepisów prawa;
  - żądania ograniczenia przetwarzania danych osobowych – w przypadku gdy:
  - osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych,
  - przetwarzanie danych jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych, żądając w zamian ich ograniczenia,
  - Administrator nie potrzebuje już danych dla swoich celów, ale osoba, której dane dotyczą, potrzebuje ich do ustalenia, obrony lub dochodzenia roszczeń,
  - osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania danych – do czasu ustalenia, czy prawnie uzasadnione podstawy po stronie Administratora są nadrzędne wobec podstawy sprzeciwu;
  - przenoszenia danych osobowych – w przypadku gdy:
  - przetwarzanie odbywa się na podstawie umowy zawartej z osobą, której dane dotyczą lub na podstawie zgody wyrażonej przez taką osobę oraz
  - przetwarzanie odbywa się w sposób zautomatyzowany;
  - sprzeciwu wobec przetwarzania danych osobowych, w tym profilowania, gdy zaistnieją przyczyny

związane z Państwa szczególną sytuacją, a przetwarzanie danych oparte jest na podstawie niezbędności do celów wynikających z prawnie uzasadnionego interesu.
W przypadku przetwarzania danych na podstawie zgody osoby, której dane dotyczą, przysługuje prawo do cofnięcia zgody. Cofnięcie zgody nie ma wpływu na zgodność z prawem przetwarzania danych, którego dokonano na podstawie zgody przed jej wycofaniem.
Osobie, która uzna, że przetwarzanie jej danych osobowych narusza przepisy Rozporządzenia RODO przysługuje prawo wniesienia skargi do organu nadzorczego - **Prezes Urzędu Ochrony Danych Osobowych**

Załącznik nr 8
do Polityki Bezpieczeństwa Informacji
w Domu Pomocy Społecznej „SENIOR”
im. Jana Kaczmarka w Czeladzi

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

.

Lp.	**Dokładny adres** *(np. adres siedziby firmy gdzie przetwarzane są dane)*	**Dział użytkujący pomieszczenie**	**Nr pokoju lub pomieszczenia**	**Rodzaj zastosowanego zabezpieczenia pomieszczenia**	**Uwagi**

Data i podpis Administratora Bezpieczeństwa Informacji

….....

Załącznik nr 9
do Polityki Bezpieczeństwa Informacji
w Domu Pomocy Społecznej „SENIOR”
im. Jana Kaczmarka w Czeladzi

ANALIZA RYZYKA I ZAGROŻEŃ w DOMU POMOCY SPOŁECZNEJ „SENIOR”

im. Jana Kaczmarka w Czeladzi

Analiza ryzyka i zagrożeń stworzona została z uwagi na wzrost zagrożeń dla bezpieczeństwa informacji, w szczególności rosnąca cyberprzestępczość oraz zmieniające się przepisy prawne, wymagają od Administratora Danych Osobowych prowadzenia regularnego szacowania ryzyka oraz metod zabezpieczania danych chronionych. Głównym elementem procesu zarządzania ryzykiem bezpieczeństwa informacji jest analiza ryzyka, której celem jest identyfikacja zasobów, odpowiadających im podatności i zagrożeń, a także oszacowanie prawdopodobieństwa ich wystąpienia oraz wielkości potencjalnych strat.

Na przeprowadzenie analizy ryzyka i zagrożeń składają się:

1. Szacowanie ryzyka
2. Identyfikacja i ocena zasobów chronionych
3. Identyfikacja podatności zasobów chronionych na zagrożenia
4. Identyfikacja zagrożeń

Identyfikacja i ocena zasobów chronionych nie związanych z TI

W przeprowadzonej analizie skupiono się na zasobach nie związanych z teleinformatyką. Zasoby mające związek z teleinformatyką DPS zawarte zostały w dokumencie (zarządzenie ryzykiem informatycznym). Określenie pozostałych zasobów chronionych w DPS pozwala określić zakres niskiego i wysokiego ryzyka utraty integralności, poufności i rozliczalności dla tych zasobów.

Na zasoby chronione w DPS składają się:

1. **Informacje chronione**
   1) Dane osobowe
   2) Informacje chronione umownie
2. **Procesy przetwarzania informacji**
   1) Zbieranie
   2) Modyfikowanie
   3) Utrwalanie
   4) Organizowanie
   5) Porządkowanie
   6) Przechowywanie
   7) Pobieranie
   8) Przeglądanie
   9) Wykorzystywanie
   10) Rozpowszechnianie
   11) Udostępnianie
   12) Usuwanie
   13) Niszczenie
   14) Przesyłanie

Kluczowymi zasobami, wymagającymi szczególnej ochrony są:

1. Dane osobowe;
2. Przesyłanie, udostępnienie oraz niszczenie informacji chronionych;

3. Obszary przetwarzania, poza DPS
4. Struktura organizacyjna DPS;

Identyfikacja zagrożeń

Zagrożenia można podzielić na związane z:

1. Bezpieczeństwem fizycznym
2. Bezpieczeństwem prawnym
3. Bezpieczeństwem osobowo-organizacyjnym

Najistotniejsze zagrożenia z zakresu bezpieczeństwa fizycznego:

1. Nieumiejętne przechowywanie danych papierowych
2. Nieumiejętne przechowywanie elektronicznych nośników informacji
3. Nieumiejętne niszczenie elektronicznych nośników informacji
4. Brak niszczarek
5. Brak podtrzymywanie energii urządzeń informatycznych
6. Nieuprawniony dostęp do pomieszczeń
7. Przebywanie w pomieszczeniach osób nieupoważnionych bez nadzoru
8. Niewystarczające zabezpieczenia przeciwpożarowe
9. Niewystarczające zabezpieczenia antykradzieżowe
10. Klęski żywiołowe
11. Nieumiejętna ochrona fizyczna zasobów
12. Nieumiejętne ustawienie sprzętu
13. Niedokładna inwentaryzacja sprzętu

Zagrożenia z zakresu bezpieczeństwa prawnego dla DPS:

1. Słabe identyfikowanie przepisów mających zastosowanie dla bezpieczeństwa informacji
2. Niedostateczne śledzenie zmian w przepisach
3. Powolne dostosowanie się do zmian w przepisach
4. Niedostateczne szkolenia personelu
5. Nieodpowiednia wiedza osób zaangażowanych w proces przetwarzania
6. Brak wsparcia ze strony osób świadczących obsługę prawną
7. Słaba kontrola zapisów umownych
8. Słaba kontrola legalności przetwarzania danych
9. Brak realizowania obowiązków informacyjnych
10. Niedostateczne respektowanie praw osób, których dane dotyczą
11. Unikanie zgłaszania incydentów do rejestru naruszeń

Zagrożenia z zakresu bezpieczeństwa organizacyjno-osobowego:

1. Niedostatecznie skuteczne szkolenia personelu
2. Nieodpowiednia wiedza osób zaangażowanych w proces przetwarzania
3. Nieumiejętne niszczenie danych lub dokumentów
4. Nieodpowiedni nadzór nad bezpieczeństwem informacji
5. Niefrasobliwe rozmowy
6. Słabe zaangażowanie w proces zabezpieczania danych
7. Otwieranie korespondencji mailowej od niezaufanych nadawców
8. Udostępnianie danych osobom nieupoważnionym

9. Dopuszczanie do przetwarzania osób nieupoważnionych

10. Niedostateczne zaznajomienie personelu z zasadami bezpieczeństwa informatycznego obowiązującego w DPS

11. Nieprzestrzeganie zasad bezpieczeństwa informatycznego obowiązującego w DPS

12. Brak aktualizacji dokumentacji Polityki Bezpieczeństwa

13. Brak wyznaczenia osób odpowiedzialnych za nadzór nad bezpieczeństwem

14. Wynoszenie służbowych danych poza obszar DPS

15. Zgubienie nośników informacji

16. Kradzież nośników informacji

17. Kradzież dokumentów

18. Wyrzucanie dokumentów do śmieci bez zniszczenia

19. Kradzież sprzętu komputerowego

20. Udostępnianie haseł innym osobom

Zagrożenia można też podzielić na wewnętrzne oraz zewnętrzne, a także umyślne i nieumyślne.

Wśród wewnętrznych, umyślnych działań, które powinny skutkować karami dyscyplinarnymi należy wyróżnić:

1. Niefrasobliwe rozmowy

2. Wyrzucenie dokumentów do śmieci bez zniszczenia

3. Udostępnianie haseł innym osobom

4. Wynoszenie służbowych danych (bez zgody ADO) poza obszar DPS

5. Dopuszczanie do przetwarzania osób nieupoważnionych

6. Otwieranie korespondencji mailowej od niezaufanych nadawców

7. Udostępnianie danych osobom nieupoważnionym

8. Brak nadzoru nad zgodnością przetwarzania danych z przepisami

9. Dostęp do pomieszczeń osób nieuprawnionych

10. Przebywanie w pomieszczeniach osób nieupoważnionych bez nadzoru

Są to zagrożenia, które można minimalizować poprzez ustanowienie odpowiednich zasad organizacyjnych oraz przeprowadzenie regularnych szkoleń z bezpieczeństwa informacji.

Wśród działań, które można uznać za skutkujące zaniedbaniem, wyróżnia się:

1. Brak lub nieaktualność oprogramowania antywirusowego
2. Przyznawanie użytkownikom uprawnień administratora
3. Brak inwentaryzacji zasobów
4. Nieregularne tworzenie kopii zapasowych
5. Błędna konfiguracja
6. Nieaktualne oprogramowanie
7. Brak niszczarek
8. Nieumiejętne ustawienie sprzętu
9. Nieodpowiednia wiedza osób zaangażowanych w proces przetwarzania

Analiza zagrożeń i ryzyka

Zagrożenia dla bezpieczeństwa danych przetwarzanych w systemach informatycznych można podzielić ze względu na ich charakter:

1. fizyczny – kradzież i/lub zniszczenie sprzętu komputerowego, nośników lub wydruków zawierających dane osobowe; do tej grupy zagrożeń należy zaliczyć również te, które wynikają z niszczenia zabezpieczeń fizycznych pomieszczeń (np. włamania), jak i te wynikające z nieuprawnionego dostępu do systemu informatycznego (dotyczy to włamań do sieci komputerowych i systemów przesyłania informacji);

2. losowy – wyładowania elektryczne, pożar, zalanie wodą pomieszczeń w których odbywa się przetwarzanie danych/lub są przechowywane nośniki informacji oraz wydruki komputerowe; awarie zasilania, zakłócenia w sieci energetycznej;

3. wadliwej pracy systemów informatycznych – uszkodzenia i awarie sprzętu komputerowego, nieprawidłowa praca systemów operacyjnych i/lub oprogramowania użytkowego, wirusy komputerowe, awarie sieci komputerowych (np. przydział uprawnień, dostęp do informacji, przesyłanie danych);

4. dostęp osób nieuprawnionych – brak nadzoru nad pomieszczeniami, podgląd informacji na ekranie, zła organizacja formatek ekranów (na jednym ekranie mogą być informacje dotyczące tylko jednej osoby), zły obieg dokumentów i wydawnictw, brak nadzoru nad naprawami i konserwacją sprzętu i oprogramowania, włamania do systemów informatycznych (np. przez Internet), nieprzestrzeganie zasad eksploatacji systemów komputerowych, niewłaściwy nadzór nad niszczeniem dokumentów lub kasowaniem informacji;

5. działania użytkowników – pomyłki w trakcie przetwarzania danych, kradzież i/lub nielegalne kopiowanie danych, wykorzystywanie systemów informatycznych do celów niezgodnych z przeznaczeniem.

Środki techniczne i organizacyjne służące zapewnieniu poufności, integralności i rozliczalności przetwarzania danych

Zabezpieczanie zbiorów danych osobowych przetwarzanych w systemach informatycznych, w kartotekach, księgach, wykazach itp. rejestrach, polega przede wszystkim na zastosowaniu mechanizmów kontroli dostępu i prawidłowej organizacji pracy, kontrolowaniem obiegu dokumentów, jak również zabezpieczaniu miejsc, w których przetwarza się dane osobowe i przechowuje się dokumenty oraz nośniki informacji.

Dla zapewnienia integralności i poufności przetwarzania w ramach posiadanych zasobów środki bezpieczeństwa podzielono na trzy grupy:

1. <u>Środki ochrony fizycznej</u>

   a) zbiory danych osobowych przechowywane są w pomieszczeniach zabezpieczonych drzwiami, zamykanych na klucz, jeśli w pomieszczeniu nie przebywają osoby zatrudnione przy przetwarzaniu danych osobowych,

   b) pomieszczenia Domu Pomocy Społecznej „SENIOR” im. Jana Kaczmarka w Czeladzi wyposażone są w system alarmowy przeciwwłamaniowy, który przez całą dobę monitorowany jest przez zewnętrzną służbę ochrony,

   c) zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej szafie,

   d) kopie awaryjne oraz hasła do systemów przetwarzających zbiory danych osobowych przechowywane są w zamkniętych metalowych szafach,

   e) pomieszczenia Domu Pomocy Społecznej „SENIOR” im. Jana Kaczmarka w Czeladzi zabezpieczone są przed skutkami pożaru za pomocą wolno stojących gaśnic, dodatkowo za pomocą hydrantu wewnętrznego, funkcjonuje system monitorowania przeciwpożarowego,

   f) dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

2. <u>Środki ochrony technicznej (środki sprzętowe infrastruktury informatycznej)</u>

   a) dostęp do systemu operacyjnego komputera w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła,

   b) zastosowane zostały środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie,

3. <u>Środki ochrony organizacyjnej</u>

a) osoby zatrudnione przy przetwarzaniu danych osobowych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych,
b) przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego,
c) osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązane zostały do zachowania ich w tajemnicy,
d) prowadzona jest ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych metodami tradycyjnymi oraz w systemie informatycznym,
e) określony został zakres przetwarzania danych osobowych dla każdej z osób zatrudnionych przy przetwarzaniu danych osobowych w systemie informatycznym oraz wpisany do ich indywidualnego zakresu czynności,
f) wydane zostało imienne upoważnienie dla osób zatrudnionych przy przetwarzaniu danych osobowych, w którym określa się nazwę i rodzaj zbioru czy programu przetwarzającego dane osobowe oraz termin ważności tego upoważnienia,
g) określony został sposób przydziału identyfikatorów i haseł dla użytkowników systemu informatycznego przetwarzającego dane osobowe oraz częstotliwość zmiany haseł,
h) określone zostały procedury rozpoczęcia, zawieszenia i zakończenia pracy,
i) określone zostały procedury wykonywania kopii bezpieczeństwa, sposobu ich przechowywania i sprawdzenia pod kątem jej użyteczności, wyznaczone zostały osoby odpowiedzialne za te czynności,
j) określone zostały procedury sprawdzania, usuwania wirusów komputerowych, aktualizacji bazy wirusów oraz wyznaczone zostały osoby odpowiedzialne za te czynności,
k) określone zostały procedury dokonywania przeglądu, konserwacji i likwidacji urządzeń komputerowych zawierających dane osobowe,
l) określone zostały procedury dokonywania przeglądu, napraw i likwidacji zbiorów danych osobowych w systemie informatycznym,
m) monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.

Ryzyka dla kluczowych zasobów chronionych

Zasoby chronione	**Najistotniejsze zagrożenia dla wskazanych zasobów**						
Dane osobowe	Niewłaściwe niszczenie	Niedostatecznie skuteczne szkolenia personelu	Nieumiejętne przechowywanie danych	Przechwycenie danych podczas teletransmisji	Problem z odzyskiwaniem danych z kopii zapasowych	Otwieranie korespondencji mailowej od niezaufanych nadawców	Udostępnianie haseł innym osobom
Przesyłanie, udostępnianie oraz niszczenie informacji chronionych	Niewłaściwe niszczenie	Niedostatecznie skuteczne szkolenia personelu	Przechowywanie danych podczas teletransmisji	Udostępnienie haseł innym osobom	Nieodpowiednia wiedza osób zaangażowanych w proces przetwarzania	Udostępnianie danych osobom nieupoważnionym	Wyrzucanie dokumentów do śmieci bez zniszczenia
Obszary przetwarzania, poza DPS	Podtrzymywanie energii urządzeń informatycznych	Utrata danych	Wyciek danych	Zgubienie nośników informacji	Kradzież nośników informacji	Nadzór nad bezpieczeństwem informacji	Brak szyfrowania danych przesyłanych metodą teletransmisji

Struktura organizacyjna DPS	Otwieranie korespondencji mailowej od niezaufanych nadawców	Niedostatecznie skuteczne szkolenia personelu	Nieodpowiednia wiedza osób zaangażowanych w proces przetwarzania	Nieodpowiedni nadzór nad bezpieczeństwem informacji	Wynoszenie służbowych danych poza obszar DPS	Udostępnianie haseł innym osobom	Dopuszczanie do przetwarzania osób nieupoważnionych

Szacowanie ryzyka

Proces szacowania ryzyka uwzględnia rodzaje wyróżnionych ryzyk w DPS:
1. Bezpieczeństwa fizycznego
2. Bezpieczeństwa prawnego
3. Bezpieczeństwa osobowo-organizacyjnego

Ryzyka dla bezpieczeństwa fizycznego – przykłady!

Ryzyko	Czym grozi wystąpienie ryzyka	Jak minimalizować ryzyko	Uwagi dodatkowe
Przechowywanie danych papierowych	Naruszenie poufności i rozliczalności danych. Naruszenie prywatności osób, których dane dotyczą, kary finansowe, w tym konieczność wypłacenia zadośćuczynienia osobom, których prywatność została naruszona, konieczność zgłoszenia incydentu do UODO, ryzyko kontroli doraźnej przeprowadzanej przez UODO.	Nie przechowywać danych w regałach Zapewnić szafy zamykane na klucz Zapewnić kontrolę nad tym kto ma dostęp do kluczy do określonych miejsc przechowywania danych.	Uwzględniać koszty zakupu odpowiednich szaf w planowanych budżetach
Przechowywanie elektronicznych nośników informacji	Naruszenie poufności i rozliczalności danych. Naruszenie prywatności osób, których dane dotyczą, kary finansowe, w tym konieczność wypłacenia zadośćuczynienia osobom, których prywatność została naruszona, konieczność zgłoszenia incydentu do UODO, ryzyko kontroli doraźnej przeprowadzanej przez UODO.	Nie przechowywać danych w regałach Zapewnić szafy zamykane na klucz Zapewnić kontrolę nad tym kto ma dostęp do kluczy do określonych miejsc przechowywania danych	Uwzględniać koszty zakupu odpowiednich szaf w planowanych budżetach

Podtrzymywanie energii urządzeń elektrycznych	Utrata ciągłości działania, ryzyko awarii	Zapewnienie UPS-ów Zapewnienie działania generatora prądu	Uwzględnianie kosztów zakupu UPS-ów, uwzględnianie zapewnienia ciągłości działania generatora prądu. Opracowanie procedury działania przypadku braku energii, ustalenie dla których zasobów, energia ma być podtrzymywana (które są kluczowe)
Dostęp do pomieszczeń osób nieuprawnionych	Naruszenie poufności i rozliczalności danych. Naruszenie prywatności osób, których dane dotyczą, kary finansowe, w tym konieczność wypłacenia zadośćuczynienia osobom, których prywatność została naruszona, konieczność zgłoszenia incydentu do UODO, ryzyko kontroli doraźnej przeprowadzanej przez UODO	Zapewnienie kontroli dostępu Zapewnienie odpowiedniej klasy zabezpieczeń Jasno określona polityka kluczy Przeszkolenie pracowników	Zapewnienie odpowiedniego poziomu wiedzy personelu
Monitoring wizyjny	Naruszenie poufności i rozliczalności danych	Zastosowanie monitoringu zwiększa szansę na zapobiegnięcie utracie danych, minimalizuje ryzyko kradzieży lub zniszczenia danych	Obrazy z kamer wyświetlane w trybie rzeczywistym na wydzielonym stanowisku bez dostępu osób trzecich

Ryzyka dla bezpieczeństwa prawnego

Ryzyko	Czym grozi wystąpienie ryzyka	Jak minimalizować ryzyko	Uwagi dodatkowe
Identyfikowanie przepisów mających zastosowanie dla bezpieczeństwa informacji	Zastosowaniem nieodpowiednich środków ochrony, karami administracyjnymi	Wskazanie osoby odpowiedzialnej za te czynności Inwestowanie w szkolenie osoby odpowiedzialnej za nadzór nad przepisami Współpraca z radcą prawnym	W DPS ryzyko jest identyfikowane na bieżąco
Odpowiednia wiedza osób zaangażowanych w proces przetwarzania	Nieodpowiednie zachowanie, niefrasobliwe rozmowy, wyciek danych, nie niszczenie danych, nie	Ustalenie częstotliwości przeprowadzania szkoleń	Konieczne przeprowadzenie regularnych szkoleń

	zabezpieczanie danych		
Kontrola zapisów umownych	Niewłaściwe zapisy umowne, brak umów powierzenia, brak przesłanek legalności, złamanie przepisów o ochronie danych osobowych	Współpraca z radcą prawnym Regularna kontrola zapisów umownych Zastosowanie standardowych zapisów	
Realizowanie obowiązków informacyjnych	Złamanie przepisów o ochronie danych osobowych, naruszenie prawi osób, których dane dotyczą, kary wynikające z przepisów (grzywna, ograniczenie lub pozbawienie wolności), możliwa kontrola UODO	Przeprowadzanie regularnych sprawdzeń Przeszkolenie osób pracujących przy przetwarzaniu danych Zastosowanie standardowych zapisów	

Ryzyka osobowo-organizacyjne

Szkolenia personelu	Ryzyko utraty lub wycieku danych, ryzyko udostępnienia danych osobom nieupoważnionym, ryzyko kar wynikających z ustawy, ryzyko naruszenia praw osób, których dane dotyczą	Wskazanie osoby odpowiedzialnej za te czynności Ustalenie częstotliwości przeprowadzania szkoleń	
Nadzór nad bezpieczeństwem informacji	Ryzyko utraty kontroli nad integralnością, rozliczalnością i poufnością danych	Wyznaczenie odpowiednich osób do nadzoru Zapewnienie tym osobom niezależności w swoich działaniach	IOD przeprowadza regularne sprawdzenia
Niefrasobliwe rozmowy	Ryzyko udostępnienia danych osobom nieupoważnionym, ryzyko utraty wizerunku instytucji	Wskazanie osoby odpowiedzialnej za zapewnienie przeszkolenia Ustalenie częstotliwości przeprowadzania szkoleń	
Otwieranie korespondencji mailowej od niezaufanych nadawców	Ryzyko utraty kontroli nad integralnością, rozliczalnością i poufnością danych	Ograniczenie uprawnień użytkowników Wskazanie osoby odpowiedzialnej za zapewnienie przeszkolenia Ustalenie częstotliwości przeprowadzania szkoleń Informowanie użytkowników o ryzykach i	Konieczne regularne przypominanie o procedurach

		konsekwencjach niewłaściwych działań	
Udostępnianie danych osobom nieupoważnionym	Ryzyko udostępnienia danych osobom nieupoważnionym, ryzyko kar wynikających z ustawy, ryzyko naruszenia praw osób, których dane dotyczą,	Wprowadzenie odpowiednich procedur organizacyjnych Wskazanie osób nadzorujących proces przetwarzania informacji Informowanie użytkowników o ryzykach i konsekwencjach niewłaściwych działań	

Załącznik nr 2
do Zarządzenia nr 3 /2019
Dyrektora Domu Pomocy Społecznej„SENIOR”
im. Jana Kaczmarka w Czeladzi
z dnia 15 marca 2019 r.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Domu Pomocy Społecznej „SENIOR” im. Jana Kaczmarka w Czeladzi

1. Ilekroć w niniejszej instrukcji jest mowa o::
   1) RODO – należy przez to rozumieć Rozporządzenie 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 praz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych osobowych)
   2) Rozporządzeniu - należy przez to rozumieć rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. nr 100, poz.1024);
   3) ADO – administrator danych osobowych,
   4) IOD – inspektor ochrony danych,
   5) ASI – administrator systemu informatycznego – rozumie się przez to osobę posiadającą uprawnienia do zarządzania zasobami sieci i systemów informatycznych (całymi lub wydzielonymi),
   6) Kierownik – dyrektor, w której przetwarzane są dane osobowe.
2. Do zabezpieczeń danych osobowych w Domu Pomocy Społecznej „SENIOR” im. Jana Kaczmarka w Czeladzi zwanego dalej DPS, zastosowanie mają przepisy rozporządzenia dotyczące poziomu wysokiego, a w szczególnych przypadkach mogą mieć zastosowanie zabezpieczenia poziomu podstawowego i podwyższonego.

Rozdział I.
Osoby przetwarzające dane osobowe

1. Realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych wyznacza się osoby odpowiedzialne za bieżącą realizację tej polityki na terenie DPS. Za realizację polityki bezpieczeństwa odpowiadają w szczególności:
   1) dyrektor - jako administrator danych osobowych (ADO) w rozumieniu art. 24 RODO,
   2) inspektor ochrony danych w rozumieniu art. 37 RODO
   3) inne osoby mające dostęp do danych osobowych w systemach informatycznych.
2. Osoby upoważnione do przetwarzania danych osobowych zostają zaznajomione z zakresem informacji objętych tajemnicą w związku z wykonywaną przez siebie pracą. W szczególności są one informowane o powinności zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia.
3. W przypadku naruszenia zasad bezpiecznego i zgodnego z prawem przetwarzania danych osobowych przez osoby zatrudnione w ramach stosunku pracy upoważnione do przetwarzania takich danych, działanie takie traktowane będzie jako ciężkie naruszenie podstawowych obowiązków pracowniczych z wszystkimi wynikającymi stąd konsekwencjami, z rozwiązaniem stosunku pracy włącznie.

Rozdział II.
Nadawanie uprawnień do przetwarzania danych i rejestrowanie tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

1. Dane osobowe w systemach informatycznych może przetwarzać wyłącznie osoba posiadająca stosowne upoważnienie do przetwarzania danych osobowych udzielone przez ADO. Wzór

upoważnienia do przetwarzania danych osobowych stanowi załącznik nr 3 do obowiązującej w DPS „*Polityki bezpieczeństwa informacji”.*

2. IOD prowadzi rejestr osób upoważnionych do przetwarzania danych osobowych w DPS, zgodnie z załącznikiem nr 4 do „*Polityki bezpieczeństwa informacji”.* Kopie upoważnień w odniesieniu do pracowników danej jednostki organizacyjnej przechowywane są przez kierownika tej jednostki.
3. Upoważnienie do przetwarzania danych osobowych może zostać cofnięte przed terminem jego wygaśnięcia. Pracownik powinien o tym fakcie zostać pisemnie poinformowany.
4. Fakt cofnięcia upoważnień do przetwarzania danych osobowych jest odnotowywany w rejestrze, o którym mowa w ust. 2.
5. Osoby upoważnione do przetwarzania danych osobowych gromadzonych w zasobach sieci administracyjnej posiadają indywidualne konto.

Rozdział III.
Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

1. Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie użytkownik po podaniu identyfikatora i właściwego hasła.
2. Identyfikator (login) jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik odpowiedzialny jest za wszystkie czynności wykonane przy użyciu identyfikatora, którym się posługuje lub posługiwał.
3. Na potrzeby administrowania systemem tworzone są uniwersalne konta administracyjne typu „admin”.
4. Identyfikatory i hasła kont administracyjnych typu ”admin” są przechowywane w zamkniętej szafie, do której dostęp jest w pełni kontrolowany, przy czym dostęp do szafy mają wyłącznie dyrektor DPS oraz osoby przez niego upoważnione. Identyfikatory oraz hasła osób uprawnionych do wykonywania prac administracyjnych oraz użytkowników są przechowywane w oznakowanej i podpisanej kopercie.
5. W przypadku konieczności awaryjnego użycia nazw i haseł tych użytkowników konieczne jest udokumentowanie zaistniałej sytuacji poprze dokonanie wpisu w „Dzienniku haseł”, który znajduje się w tej samej szafie, w której znajduje się koperta z hasłami użytkowników.

Rozdział IV.
Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

1. Przed rozpoczęciem oraz w trakcie pracy każdy pracownik obowiązany jest do zwrócenia szczególnej uwagi, czy nie wystąpiły przesłanki mogące świadczyć o naruszeniu ochrony danych osobowych.
2. O naruszeniu ochrony danych osobowych mogą świadczyć następujące przesłanki:
   1) brak możliwości uruchomienia przez użytkownika aplikacji pozwalającej na dostęp do danych osobowych,
   2) brak możliwości zalogowania się do tej aplikacji,
   3) ograniczone, w stosunku do normalnej sytuacji, uprawnienia użytkownika w aplikacji (na przykład brak możliwości wykonania pewnych operacji normalnie dostępnych użytkownikowi) lub uprawnienia poszerzone w stosunku do normalnej sytuacji,
   4) wygląd aplikacji inny niż normalnie,
   5) inny zakres danych niż normalnie dostępny dla użytkownika,
   6) znaczne spowolnienie działania systemu informatycznego,
   7) pojawienie się niestandardowych komunikatów generowanych przez system informatyczny,
   8) ślady włamania lub prób włamania do obszaru, w którym przetwarzane są dane osobowe,
   9) ślady włamania lub prób włamania do pomieszczeń, w których odbywa się przetwarzanie danych osobowych, w szczególności do serwerowni oraz do pomieszczeń, w których przechowywane są nośniki kopii zapasowych,
   10) włamanie lub próby włamania do szafek, w których przechowywane są –w postaci elektronicznej lub papierowej – nośniki danych osobowych,
   11) zagubienie bądź kradzież nośnika danych osobowych,

12) zagubienie bądź kradzież nośnika materiału kryptograficznego (karty mikroprocesorowej, dyskietki itp.),
13) kradzież sprzętu informatycznego, w którym przechowywane są dane osobowe,
14) informacja z systemu antywirusowego o zainfekowaniu systemu informatycznego wirusami,
15) fizyczne zniszczenie lub podejrzenie zniszczenia elementów systemu informatycznego przetwarzającego dane osobowe na skutek przypadkowych lub celowych działań albo zaistnienia działania siły wyższej,
16) podejrzenie nieautoryzowanej modyfikacji danych osobowych przetwarzanych w systemie informatycznym.

3. Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione.
4. Maksymalna liczba prób wprowadzenia hasła przy logowaniu się do systemu wynosi trzy.
5. Odblokowania konta może dokonać administrator systemu informatycznego w porozumieniu z kierownikiem jednostki.
6. W przypadku bezczynności użytkownika na stacji roboczej przez okres dłuższy niż 30 minut automatycznie włączany jest program do wygaszania ekranu.
7. Hasło powinno składać się z co najmniej 8 znaków, powinno zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.
8. Niedopuszczalne jest, aby dwóch lub większa liczba użytkowników wykorzystywała wspólnie jedno konto użytkownika.
9. W pomieszczeniach, w których przetwarzane są dane osobowe i w których jednocześnie mogą przebywać osoby postronne, monitory stanowisk dostępu do danych powinny być ustawione w taki sposób, aby uniemożliwić tym osobom wgląd w dane.
10. Prawidłowe zakończenie pracy użytkownika w systemie informatycznym obejmuje wylogowanie się użytkownika z aplikacji.

Rozdział V.
Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

1. Dane osobowe przetwarzane w systemie informatycznym podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych.
2. Za proces tworzenia kopii zapasowych na serwerach odpowiada administrator ADM.
3. Kopie zapasowe przechowuje się w miejscach zabezpieczających przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem w pomieszczeniu zamkniętym.
4. Kopie zapasowe usuwa się niezwłocznie po ustaniu ich użyteczności.

Rozdział VI.
Sposób, miejsce i okres przechowywania nośników informacji zawierających dane osobowe oraz kopii zapasowych

1. Nośniki danych zarówno w postaci elektronicznej, jak i papierowej powinny być zabezpieczone przed dostępem osób nieuprawnionych, nieautoryzowaną modyfikacją i zniszczeniem.
2. Ewentualne wydruki (dane w postaci papierowej) powinny być przechowywane w zamkniętych szafach wewnątrz obszaru przeznaczonego do przetwarzania danych osobowych i nie powinny być bez uzasadnionej przyczyny wynoszone poza ten obszar.
3. W przypadku, gdy nośnik danych osobowych nie jest już potrzebny, należy przeprowadzić zniszczenie nośnika lub usunięcie danych z nośnika - tak, by danych tych nie można było przypisać konkretnej lub dającej się ustalić osobie lub by konieczny był w tym celu nieproporcjonalnie duży nakład czasu, kosztów i pracy.
4. Jeżeli wydruk danych osobowych nie jest już potrzebny, należy przeprowadzić zniszczenie wydruku przy użyciu niszczarki dokumentów.

Rozdział VII.
Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

1. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.
2. Prace serwisowe są wykonywane wyłącznie przez uprawniony podmiot lub przez upoważnionych przedstawicieli wykonawców zewnętrznych.
3. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
   1) likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,
   2) przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie,
   3) naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej.
4. Wszelkie przeglądy i konserwacje stacji roboczych wykonywane są na bieżąco. Przeglądy i konserwacje serwerów wykonywane są nie rzadziej niż raz na 3 miesiące.

Rozdział VIII.
Postępowanie w przypadku naruszenia ochrony danych osobowych

1. W przypadku wystąpienia naruszeniem zabezpieczenia systemu informatycznego należy postępować zgodnie z procedurą zarządzania incydentami – Załącznik nr 1 do niniejszej Instrukcji zarządzania systemem informatycznym.

Rozdział IX.
Uwagi końcowe

1. Wszystkie osoby zaangażowane w procesy przetwarzania danych osobowych (w tym przetwarzanie w systemie informatycznym) w DPS, bez względu na zajmowane stanowisko i miejsce wykonywania pracy oraz charakter stosunku pracy, są zobowiązane do postępowania zgodnie z zasadami określonymi w niniejszej Instrukcji.
2. Nieprzestrzeganie zasad postępowania określonych w niniejszej Instrukcji stanowi naruszenie obowiązków pracowniczych i może być przyczyną zastosowania odpowiednich sankcji wynikających z odpowiedzialności dyscyplinarnej określonej w Kodeksie Pracy.
3. Jeżeli skutkiem działania lub zaniechania osoby upoważnionej do przetwarzania danych osobowych stanowiących zasoby DPS jest ujawnienie danych osobie nieuprawnionej, sprawca może zostać pociągnięty do odpowiedzialności karnej wynikającej z Kodeksu Karnego.
4. Jeżeli skutkiem działania lub zaniechania osoby upoważnionej do przetwarzania danych osobowych stanowiących zasoby DPS jest szkoda, sprawca ponosi odpowiedzialność materialną na warunkach określonych w przepisach Kodeksu Pracy oraz Kodeksu Cywilnego i innych przepisów szczególnych znajdujących zastosowanie.
5. ADO zapewnia środki organizacyjne, techniczne i finansowe na realizację zadań wynikających z niniejszej instrukcji.

Załącznik nr 1
do Instrukcji Zarządzania systemem Informatycznym
służącym do przetwarzania danych osobowych
w Domu Pomocy Społecznej „SENIOR”
im. Jana Kaczmarka w Czeladzi

PROCEDURA ZARZĄDZANIA INCYDENTAMI

1. Cel procedury.

Celem Procedury Zarządzania Incydentami Związanymi z Bezpieczeństwem Informacji jest zapewnienie, że zdarzenia związane z bezpieczeństwem informacji oraz słabości systemów informacyjnych, są zgłaszane w sposób umożliwiający szybkie podjęcie działań korygujących.

2. Zakres stosowania.

Działania opisane w niniejszej procedurze obowiązują, we wszystkich komórkach organizacyjnych Domu Pomocy Społecznej „SENIOR” im. Jana Kaczmarka w Czeladzi z siedzibą w Czeladzi przy ul. Szpitalnej 5A.

3. Odpowiedzialność.

Odpowiedzialność za prawidłowe zgłoszenie incydentów dotyczących bezpieczeństwa infrastruktury informatycznej spoczywa na pracownikach dokonujących zgłoszeń. Informatyk odpowiedzialny jest za rozwiązanie problemu lub zapobieżenie incydentowi działając zgodnie z niniejszą procedurą.

Informatyk jest odpowiedzialny za:

1) Niezwłoczne reagowanie na incydenty bezpieczeństwa informacji w określony i z góry ustalony sposób;
2) Ocenę istniejących i potencjalnych zagrożeń w zakresie bezpieczeństwa informacji;
3) Ocenę przyczyn i skutków incydentów naruszenia bezpieczeństwa informacji w tym gromadzenie materiału dowodowego;
4) Przygotowywanie propozycji działań korygujących i naprawczych oraz nadzór nad ich wprowadzaniem;
5) Dokonywanie okresowego przeglądu i aktualizacji Polityki Bezpieczeństwa Informacji;
6) Prowadzenie działań zmierzających do wzrostu świadomości w zakresie zapewnienia bezpieczeństwa informacji;

4. Klasyfikacja incydentów.

Podział zdarzeń:

Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji

1) Zdarzenia losowe zewnętrzne (np.: klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej, ciągłość pracy systemów zostaje zakłócona, nie dochodzi do naruszenia poufności danych.

2) Zdarzenia losowe wewnętrzne (np.: niezamierzone pomyłki administratorów, awarie sprzętowe, błędy w oprogramowaniu), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.

3) Zdarzenia zamierzone, świadome i celowe - stanowią najpoważniejsze zagrożenie naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zdarzenia te możemy podzielić na:

• nieuprawniony dostęp do danych z zewnątrz (włamanie do systemu),

• nieuprawniony dostęp do danych z sieci wewnętrznej,

• nieuprawniony transfer danych,

• pogorszenie funkcjonowania sprzętu i oprogramowania (np.: działanie wirusów),

• bezpośrednie zagrożenie materialnych składników systemu (np.: kradzież sprzętu).

Przykłady zdarzeń które mogą być zakwalifikowane jako uzasadnione podejrzenie naruszenia bezpieczeństwa informacji:

1) Sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na infrastrukturę teleinformatyczną jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.

2) Niewłaściwe parametry środowiska jak zbyt wysoka temperatura lub nadmierna wilgotność (w szczególności dotyczy to serwerowni).

3) Awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie systemu, a w tym sam fakt pozostawienia serwisantów bez nadzoru.

4) Pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu.

5) Jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikacje w systemie.

6) Nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie.

7) Stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji).

8) Nastąpiła niedopuszczalna manipulacja danymi w systemie.

9) Ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą elementy systemu zabezpieczeń.

10) Praca w systemie lub w sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych, np.: praca w systemie lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.

11) Ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki", itp.

12) Podmieniono lub zniszczono nośniki z danymi bez odpowiedniego upoważnienia lub w niedozwolony sposób skasowano lub kopiowano dane osobowe.

13) Rażąco naruszono dyscyplinę pracy w zakresie przestrzegania PBI (nie wylogowanie się, pozostawienie włączonego komputera po zakończeniu pracy, nie zamknięcie pokoju z komputerem, nie wykonywanie w ustalonych terminach kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.)

14) Stwierdzenie nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych, w tym także osobowych (otwarte szafy, regały, biurka).

5. Zgłaszanie incydentów

Pracownicy Domu Pomocy Społecznej „SENIOR” im. Jana Kaczmarka w Czeladzi mają obowiązek zgłaszać zauważone przez siebie incydenty oraz notować wszystkie szczegóły związane z incydentem.

Incydenty można zgłaszać mailem: wiejak.agnieszka098@gmail.com lub telefonicznie: 600-145-852

Zgłoszenie musi zawierać:

• imię i nazwisko zgłaszającego,
• miejsce i datę wystąpienia incydentu,
• opis zdarzenia.

Zgłaszający incydent nie powinien podejmować żadnych działań na własną rękę jednak w miarę możliwości powinien zabezpieczyć materiał dowodowy, np.: robiąc zdjęcie ekranu komputera co do którego zaistniało podejrzenie, że jego działanie odbiega od normy.

6. Postępowanie z incydentami

Obsługa incydentu rozpoczyna się od jego dokładnego rozpoznania - ustalenia oznak naruszenia bezpieczeństwa, identyfikacji rodzaju incydentu, identyfikacji i zabezpieczenia dowodów oraz poinformowania o zdarzaniu odpowiednich osób.

1) IOD, który przyjął zgłoszenie, powiadamia niezwłocznie ADO lub osobę go zastępującą o fakcie i treści zgłoszenia.

2) Po analizie zdarzenia i okoliczności z nim związanych Informatyk wprowadza dane o incydencie do rejestru incydentów oraz zabezpiecza materiał dowodowy. Zawiadamia IOD oraz ADO.

3) ADO wraz IOD zbiera się niezwłocznie, dokonuje analizy materiału dowodowego i podejmuje decyzję o sposobie dalszego postępowania. Gromadzenie materiału dowodowego: dla dokumentów papierowych: oryginał jest bezpiecznie przechowywany wraz z informacją, kto znalazł dokument, gdzie, kiedy i kto by był świadkiem tego zdarzenia; każde śledztwo może wykazać, że oryginał nie został naruszony dla dokumentów na nośnikach komputerowych zaleca się: utworzenie obrazu lub kopii (zależnie od stosownych wymagań) wszelkich nośników wymiennych; zaleca się zapisanie informacji znajdujących się na dyskach twardych lub w pamięci komputera, aby zapewnić ich dostępność, zaleca się zachowanie zapisów wszelkich działań podczas procesu kopiowania oraz aby proces ten odbywał się w obecności świadków; zaleca się przechowywanie oryginalnego nośnika i dziennika zdarzeń w sposób bezpieczny i nienaruszony (jeśli to niemożliwe, to co najmniej jeden obraz lustrzany lub kopię).

4) W przypadku, gdy zgłoszone zdarzenie zostało uznane za incydent bezpieczeństwa informacji, Informatyk oraz IOD dokonuje oceny istotności incydentu oraz zawiadamia ADO o zaistnieniu incydentu oraz poziomie zagrożenia dla bezpieczeństwa informacji. Informatyk ocenia poziom istotności incydentu dla DPS kierując się następującymi kryteriami:

• wpływ incydentu na ciągłość działania DPS i wypełnianie jego zadań statutowych;

• krytyczność systemów dotkniętych skutkami incydentu bezpieczeństwa;

• wrażliwość informacji, których poufność, integralność czy dostępność naruszono (na przykład czy naruszono bezpieczeństwo informacji prawnie chronionej - np.: danych osobowych, informacji niejawnych);

• rozległość wpływu incydentu na działanie systemów (nie działa jeden komputer, cała sieć itp.);

• rozmiar szkód powstałych skutkiem incydentu;

• koszt usunięcia i naprawy skutków incydentu bezpieczeństwa;

• szacowany czas przywrócenia ciągłości działania dotkniętego incydentem bezpieczeństwa systemu;

• zasoby wymagane do przywrócenia ciągłości działania systemu (personel, wsparcie firm zewnętrznych, wymagane dodatkowe czy zamienne urządzenia oraz oprogramowanie, czas odtwarzania systemów z kopii zapasowych itp.);

5) W przypadku, gdy zgłoszone zdarzenie nie zostało zaklasyfikowane jako incydent bezpieczeństwa informacji, ma charakter fałszywego alarmu ASI powiadamia zgłaszającego o zdarzeniu, że zdarzenie nie stanowi incydent bezpieczeństwa.

6) W przypadku stwierdzenia działań umyślnych i ustaleniu sprawcy incydentu zespół przekazuje wyniki analizy wraz z zabezpieczonym materiałem dowodowym ADO w celu wyciągnięcia konsekwencji dyscyplinarnych wobec sprawcy, ewentualnego zawiadomienia organów ścigania lub podjęcia kroków prawnych wobec osób trzecich.

7) IOD wraz z Informatykiem inicjują działania naprawcze zmierzające do zniwelowania szkód wyrządzonych przez incydent, wyciąga wnioski z każdego incydentu i określa jeśli to możliwe działania korygujące i zapobiegawcze w celu uniknięcia ponownego wystąpienia incydentu.

8) Na bieżąco dokumentowane są działania na każdym z etapów procesu zarządzania incydentem w formie notatki. Obsługa incydentu kończy się raportem zatwierdzonym przez IOD, Informatykiem oraz ADO zawierającym opis incydentu oraz wnioski co do działań na przyszłość.