**POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH**



 **Fundacja**

 **Domowe Hospicjum Dziecięce**

**Promyczek**

Otwock, czerwiec 2018

**§1**

**Postanowienia ogólne**

1. Polityka Bezpieczeństwa rozumiana jest jako wykaz praw, reguł i wewnętrznych praktyk regulujących sposób zarządzania i ochrony danych osobowych dla Domowego Hospicjum Dziecięcego Promyczek z siedzibą w Otwocku, ul. Narutowicza 80, 05-400 Otwock zwanej dalej Hospicjum.
2. Dokument obejmuje całokształt zagadnień związanych z problemem zabezpieczenia danych osobowych przetwarzanych zarówno tradycyjnie, jak i w systemach informatycznych. Wskazuje działania przewidziane do wykonania oraz sposób ustanowienia zasad i reguł postępowania koniecznych do zapewnienia właściwej ochrony przetwarzanych danych osobowych.

**§2**

 **Podstawa prawna**

1. Polityka Bezpieczeństwa została opracowana na podstawie:
2. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 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),
3. Ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej (t.j. z dnia 8 grudnia 2017 r. [(Dz.U. z 2018 r. poz. 160)](https://sip.legalis.pl/document-view.seam?documentId=mfrxilrtg4ytcobyhezto)
4. Ustawa z dnia 06 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (t.j. z dnia 8 czerwca 2017 r. [(Dz.U. z 2017 r. poz. 1318)](https://sip.legalis.pl/document-view.seam?documentId=mfrxilrtg4ytcmruhe3tc) ),
5. Ustawa z dnia 27 sierpnia 2004 r. o świadczeniach zdrowotnych finansowanych ze świadczeń publicznych (t.j. Dz. U. z 2017 r. poz. 1938, 2110, 2217, 2361, 2434),
6. Ustawa z dnia 21 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz. U. 2017 tj. poz.1845),
7. Pozostałe przepisy regulujące system ochrony danych osobowych, w tym przepisy wydane na podstawie art. 40 RODO.
8. Administratorem danych osobowych jest Fundacja Domowe Hospicjum Dziecięce Promyczek. Dane pacjentów Hospicjum są chronione zgodnie z polskim prawem oraz procedurami dotyczącymi bezpieczeństwa i poufności przetwarzanych danych.

**§3**

Podstawa prawna przetwarzania danych osobowych (RODO)

1. Przetwarzanie danych osobowych użytkowników odbywa się zgodnie z:

o art. 6 ust. 1 lit. a) RODO – na podstawie zgody osoby, której dane dotyczą, w

przypadku wyrażenia zgody na przetwarzanie danych w określonym celu (np.

zapisanie się na newsletter),

o art. 6 ust. 1 lit. b) RODO – w celu wykonania umowy, której stroną jest osoba,

której dane dotyczą, lub podjęcia działań przed zawarciem umowy (np.

realizacja usług świadczonych drogą elektroniczną),

o art. 6 ust. 1 lit. c) RODO – w celu wypełnienia obowiązku prawnego ciążącego

na administratorze (np. przechowywanie dokumentacji księgowej),

o art. 6 ust. 1 lit. f) RODO – w prawnie uzasadnionych interesach administratora

(np. w celu dochodzenia roszczeń)

**§4**

 **Definicje**

1. **Administrator Danych Osobowych (ADO)** – rozumie się przez to Fundację Domowe Hospicjum Dziecięce Promyczek z siedzibą w Otwocku, ul. Narutowicza 80, 05-400 Otwock.
2. **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Dane te mogą dotyczyć pracowników Hospicjum wykonującego działalność leczniczą, jego pacjentów lub osoby współpracujące z Hospicjum.
3. **Przetwarzanie danych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.
4. **Zbiór danych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów.
5. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
6. **Identyfikator użytkownika** (login) – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
7. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
8. **Uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
9. **Integralność danych** – funkcjonalność zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
10. **Poufność danych** – funkcjonalność zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom.
11. **Rozporządzenie (RODO)** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 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).

**§5**

 **Deklaracja**

1. Administrator danych mając świadomość, iż przetwarza dane wrażliwe pacjentów deklaruje dołożyć wszelkich starań, aby przetwarzanie odbywało się w zgodności z przepisami prawa.
2. Administrator deklaruje, że proces przetwarzania danych osobowych uwzględnia zasady, o których mowa w Motywie 39 RODO oraz artykule 5 ust. 1 ppkt a) – e) RODO.
3. Każdy pracownik upoważniony do przetwarzania danych, świadomy odpowiedzialności, zobowiązany jest postępować zgodnie z przyjętymi zasadami i minimalizować zagrożenia wynikające z błędów ludzkich.
4. W trosce o czytelny i uporządkowany stan materii, wprowadza się stosowne środki organizacyjne i techniczne zapewniające właściwą ochronę danych oraz nakazuje ich bezwzględne stosowanie, zwłaszcza przez osoby dopuszczone do przetwarzania danych.
5. Dane osobowe w podmiocie przetwarzane są w sposób legalny, na podstawie art. 6 ust. 1 ppkt a) i- d)oraz art. 9 ust. 2 ppkt h) RODO w związku z art. 3 ust. 1 i 2 ustawy o działalności leczniczej oraz art. 24 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, a także w związku z art. 54 ustawy o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa lub innych właściwych przepisów z zakresu prawa ubezpieczeń społecznych.
6. W przypadku konieczności pozyskania zgody na przetwarzanie danych osobowych podmiot korzysta z szablonu, którego wzór stanowi Załącznik nr 8. Zgoda na przetwarzanie danych osobowych może zostać pozyskana w inny sposób, ale musi ona spełniać przesłanki, o których mowa w art. 7 ust. 1 RODO.
7. Zakres pozyskiwanych danych wynika z przepisów prawa, o których mowa w §2 niniejszego dokumentu i jest adekwatny do zdefiniowanych celów przetwarzania.
8. Okres czasu, przez jaki dane osobowe są przetwarzane wynika z przepisów prawa, o których mowa w §2 niniejszego dokumentu. Terminy przechowywania dokumentacji medycznej określa art. 29 Ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta.

**§6**

**Wykaz zbiorów osobowych**

1. Dane osobowe przetwarzane przez ADO łączone są w zbiory, za pomocą których Administrator może ocenić ryzyko ich przetwarzania oraz ocenić konieczność przeprowadzenia procedury oceny skutków dla systemu ochrony danych, o którym mowa w art. 35 RODO.
2. Zbiory danych osobowych opisane są z uwzględnieniem poniższych informacji:
3. Nazwa zbioru,
4. Rodzaj pomieszczenia, gdzie przetwarzany jest zbiór,
5. Piętro i nr pomieszczenia,
6. Miejsce składowania danych,
7. Źródło pozyskiwania danych,
8. Programy, aplikacje służące do przetwarzania danych i sposób przepływu danych między nimi.

**§7**

 **Wykaz miejsc przetwarzania**

1. Obszarem przetwarzania danych są wszystkie pomieszczenia, korytarze oraz obszar wykonywanych świadczeń podczas wizyty domowej u Pacjenta.
2. Szczegółowy wykaz pomieszczeń w których przetwarzane są dane osobowe, stanowi załącznik nr 2 do niniejszej dokumentacji. Dla pomieszczeń, w których dane są gromadzone opisano zastosowane środki ochrony technicznej.

**§8**

 **Rejestr czynności przetwarzania**

1. Dla zbiorów, w których przetwarzane są dane, o których mowa w art. 9 ust. 1 RODO prowadzony jest rejestr czynności przetwarzania.
2. Rejestr, o którym mowa w punkcie 1 niniejszego rozdziału może być również prowadzony dla innych zbiorów lub jedna czynność przetwarzania może obejmować kilka zbiorów danych osobowych.
3. Rejestr czynności przetwarzania winien zawierać co najmniej informacje, o których mowa w art. 30 RODO tj.:
4. Imię i nazwisko lub nazwę oraz dane kontaktowe administratora;
5. cele przetwarzania;
6. opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
7. kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
8. gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń;
9. terminy usunięcia poszczególnych kategorii danych;
10. ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.
11. Rejestr czynności przetwarzania jest prowadzony w oparciu o załącznik nr 9.

**§9**

**Ewidencja osób upoważnionych do przetwarzania danych osobowych**

1. Wprowadza się ewidencję osób upoważnionych do przetwarzania danych, która stanowi załącznik nr 3 do niniejszej dokumentacji.
2. Ewidencja zawiera: imię i nazwisko osoby upoważnionej, stanowisko, datę nadania i ustania uprawnień oraz zakres, a w przypadku, kiedy dane są przetwarzane za pomocą programu komputerowego oraz identyfikator(login) dostępowy do tego programu.

**§10**

**Środki organizacyjne ochrony danych osobowych**

1. Przetwarzanie danych osobowych na terenie Hospicjum może odbywać się wyłącznie w ramach wykonywania zadań służbowych. Zakres uprawnień jest ściśle proporcjonalny do tych zadań.
2. Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych.
3. Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające nadane upoważnienie wydane przez Administratora danych osobowych. Wzór upoważnienia / unieważnienia do przetwarzania danych osobowych stanowi załącznik nr 4 do niniejszej dokumentacji.
4. Osoby przebywające i wykonujące czynności służbowe w obszarze przetwarzania danych osobowych a nie przetwarzające danych, obowiązuje zasada zachowania poufności wg załącznika nr 5 do niniejszej dokumentacji.
5. Każdy zatrudniony w Hospicjum co najmniej raz na rok musi odbyć szkolenie z zakresu ochrony danych osobowych. Nowo przyjęty pracownik odbywa szkolenie przed przystąpieniem do przetwarzania danych.
6. Każdy upoważniony do przetwarzania danych potwierdza pisemnie fakt zapoznania się z niniejszą dokumentacją i zrozumieniem wszystkich zasad bezpieczeństwa. Wzór potwierdzenia stanowi załącznik nr 6 do niniejszej dokumentacji. Podpisany dokument jest dołączany do akt osobowych pracownika lub stanowi załącznik do zawartej umowy.
7. Przebywanie osób nieuprawnionych w obszarze przetwarzania danych jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych.
8. Pomieszczenia stanowiące obszar przetwarzania danych powinny być zamykane na klucz.
9. Po zakończeniu pracy, przed opuszczeniem pomieszczenia stanowiącego obszar przetwarzania danych należy zamknąć okna oraz usunąć z biurka wszystkie dokumenty i nośniki informacji oraz umieścić je w przystosowanych do tego szafach lub biurkach z możliwością zamknięcia na klucz.
10. W podmiocie zabronione jest udzielanie wszelkich informacji zawierających dane osobowe osobom, których tożsamości nie można zweryfikować. Weryfikacja tożsamości może odbywać się poprzez żądanie okazania dokumentu tożsamości lub innego dokumentu zawierającego zdjęcie wnioskodawcy lub poprzez wykorzystanie informacji zawartej w dokumentacji medycznej, która jest znana jedynie wnioskodawcy. Do tego celu należy wykorzystać metodę pytań bezpośrednich, w których wnioskodawca udzieli poprawnych informacji w co najmniej dwóch zapytaniach.
11. W Praktyce niedopuszczalne jest przekazywania jakichkolwiek informacji zawierających dane osobowe podmiotom, instytucjom czy też organom, które nie mogą się wykazać prawidłową podstawą prawną dostępu do danych osobowych.
12. W przypadku konieczności wydania dokumentów zawierających dane osobowe (np. wynik badań, recepty itp.) należy każdorazowo weryfikować tożsamość odbierającego za pomocą mechanizmu, o którym mowa w ust.10 niniejszego artykułu, a w przypadku, kiedy odbierającym nie jest adresat dokumentu należy odnieść się do złożonego upoważnienia przez pacjenta w posiadanej przez Hospicjum dokumentacji medycznej.
13. Organizacja rejestracji i obsługi pacjenta umożliwia zachowanie poufności osobom przebywającym bezpośrednio w obszarze przetwarzania danych.
14. Udzielanie świadczeń zdrowotnych w Hospicjum odbywa się w miejscach specjalnie do tego wyznaczonych. Zabrania się udzielania informacji dotyczących pacjentów na korytarzach lub innych nieprzystosowanych do tego miejscach w Hospicjum.
15. Zabrania się eksponowania dokumentów zawierających dane osobowe w miejscach niezabezpieczonych np. biurkach, półkach, parapetach, itp.
16. Wydruki i inne dokumenty zawierające dane osobowe są przechowywane w pomieszczeniach do tego wyznaczonych. Na stanowiskach pracy mogą być dostępne jedynie dokumenty dotyczące danej sprawy/ danego pacjenta. Stosowana jest zasada tzw. czystego biurka.
17. Dokumenty zawierające dane osobowe należy niszczyć w niszczarkach lub w przypadku dużej ilości dokumentów, korzystać w tym celu z usług profesjonalnych podmiotów, zajmujących się utylizacją dokumentacji.
18. Wobec osób, których dane są przetwarzane wykonuje się obowiązek informacyjny, zgodnie z art. 12-14 RODO, a wzór klauzul informacyjnych znajduje się w załączniku nr 7.
19. Obowiązek informacyjny wobec pacjentów jest wykonywany poprzez umieszczenie na tablicy informacyjnej w biurze hospicjum oraz na stronie internetowej Hospicjum.
20. Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.
21. Dokumenty w wersji elektronicznej, które zapisywane są na nośniki zewnętrzne, przenoszone poza obszary przetwarzania lub przesyłane pocztą elektroniczną, należy zabezpieczyć poprzez nadanie im haseł odczytu.
22. Zbiory osobowe przetwarzane elektronicznie należy zabezpieczać poprzez wykonywanie kopii bezpieczeństwa, zapisywanych na zewnętrznych nośnikach i przechowywanych pod zamknięciem.
23. Komputery, które przetwarzają dane osobowe należy wyposażyć w urządzenia podtrzymujące napięcie na wypadek braku zasilania.
24. Pliki edytorów tekstu lub arkuszy kalkulacyjnych należy traktować jak kopie zbiorów, z których pochodzą przetwarzane w nich dane i odpowiednio zabezpieczać stosując wytyczne zawarte §12 Zabezpieczenie systemu informatycznego.
25. W celu zapewnienia bezpieczeństwa przetwarzanych danych elektronicznie należy zapewnić logowanie do systemu operacyjnego oraz bezpośrednio do programów przetwarzających dane.
26. Z wszystkimi współpracującymi podmiotami gospodarczymi podpisano, na mocy art. 28 RODO, umowy powierzenia przetwarzania danych osobowych wg załącznika nr 1 lub w umowach podstawowych wprowadzono uregulowania odnoszące się do obowiązków zapewnienia przestrzegania przepisów RODO przez te podmioty. W podmiocie leczniczym prowadzona jest ewidencja podmiotów, z którymi zawarto umowy powierzenia, której wzór stanowi załącznik nr 11.
27. Szczegółowe zasady postępowania ze zbiorami przetwarzanymi elektronicznie określa §12 Zabezpieczenie systemu informatycznego.

**§11**

**Udostępnianie danych**

1. Hospicjum udostępnia dane osobowe jedynie na podstawie obowiązujących przepisów prawa i w granicach prawa.
2. Dane osobowe pacjentów, które znajdują się w dokumentacji medycznej są udostępniane na zasadach, w trybie i na sposób określony w przepisach art. 26 i 27 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta.
3. Ewidencja udostępnionej dokumentacji medycznej prowadzona jest na podstawie art. 27 ust. 4 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta i zawiera, co najmniej: imię (imiona) i nazwisko pacjenta, którego dotyczy dokumentacja medyczna, sposób udostępnienia dokumentacji medycznej;, zakres udostępnionej dokumentacji medycznej, imię (imiona) i nazwisko osoby innej niż pacjent, której została udostępniona dokumentacja medyczna, a w przypadkach, o których mowa wart. 26 *udostępnianie dokumentacji medycznej* ust. 3 i 4, także nazwę uprawnionego organu lub podmiotu, imię (imiona) i nazwisko oraz podpis osoby, która udostępniła dokumentację medyczną, datę udostępnienia dokumentacji medycznej, podpis przyjmującego dokumentację medyczną.
4. Wzór wykazu, o którym mowa w ustępie 3 niniejszego paragrafu stanowi załącznik nr 10.
5. Hospicjum udostępnia również dane, na podstawie innych przepisów prawa niż te, o których mowa w ustępie 2 niniejszego paragrafu jedynie na pisemny wniosek i za potwierdzeniem wydania / odbioru.
6. Hospicjum przekazując dane drogą pocztową przekazuje je listem poleconym za potwierdzeniem odbioru.
7. W przypadku udostępniania dokumentów za pomocą korespondencji mailowej podmiot ma obowiązek szyfrować przekazywane pliki.

**§12**

 **Zabezpieczenie systemu informatycznego**

1. Obsługa i zabezpieczenie systemu informatycznego Administrator danych zleca następujący zakres zadań specjaliście IT:
2. prowadzenie monitoringu przetwarzania danych,
3. administrowanie systemem informatycznym,
4. nadawanie i aktualizowanie uprawnień użytkownikom do systemu informatycznego,
5. stosowanie środków ochrony w ramach oprogramowania użytkowego, systemów operacyjnych, urządzeń teletransmisyjnych, programów antywirusowych oraz ochrony sprzętowej,
6. kontrola mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontrola dostępu do danych osobowych,
7. kontrola systemu antywirusowego,
8. kontrola awaryjnego zasilania komputerów,
9. kontrola i wykonywanie kopii awaryjnych,
10. konserwacja oraz uaktualnienia systemów informatycznych,
11. prowadzenie ewidencji elektronicznych nośników przetwarzania danych osobowych wg załącznika nr 13
12. informowanie na bieżąco ADO o przypadkach awarii programowych wynikających z posługiwania się przez użytkowników nieautoryzowanym oprogramowaniem, nie przestrzegania zasad używania programów antywirusowych, niewłaściwego wykorzystywania sprzętu komputerowego,
13. przedstawianie Administratorowi danych, nie rzadziej niż raz na rok, kompleksowej analizy przetwarzania danych osobowych w systemem informatycznym oraz ewentualne potrzeby w zakresie zabezpieczeń.
14. Wszystkie zapisy w dokumentacji, które odwołują się do systemu informatycznego są rozumiane jako zapisy dotyczące ADO.

**§13**

**Zarządzanie ryzykiem w Hospicjum**

1. W podmiocie przeprowadzana jest analiza ryzyka. Analiza ryzyka może odbywać się dla wszystkich wyodrębnionych zbiorów danych osobowych lub dla procesów przetwarzania.
2. Analiza ryzyka przeprowadzana jest w celu określenia, oceny i minimalizacji zagrożeń, których efektem ma być wdrożenie optymalnych i adekwatnych zabezpieczeń.
3. Analiza ryzyka przeprowadzona jest corocznie, nie później niż do dnia 31 marca dla wszystkich czynności przetwarzania lub w przypadku wprowadzenia nowych procedur lub rozwiązań organizacyjnych w podmiocie leczniczym, zgodnie z odrębną procedurą przyjętą przez Praktykę.
4. Analizę ryzyka przetwarzania danych osobowych charakteryzuje załącznik nr 9.1

**§14**

1. Inspektor Ochrony Danych Osobowych

Administrator nie powołuje **Inspektora Ochrony Danych**, mając na uwadze, że:

- nie jest podmiotem publicznym

- główna działalność Administratora nie polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagałyby regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę

ani też:

- główna działalność Administratora nie polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych o szczególnym charakterze ani też danych dotyczących wyroków skazujących i naruszeń prawa.

**§15**

 **Zasady postępowania w przypadku naruszenia systemu ochrony danych**

1. Każda osoba, której Administrator wydał upoważnienie do przetwarzania danych osobowych, ma obowiązek natychmiastowego powiadamiania o występującym zagrożeniu lub wystąpieniu incydentu związanego z systemem ochrony danych osobowych w Praktyce.
2. Powiadomienie to może mieć charakter ustny lub pisemny.
3. Adresatem takiego powiadomienia jest Administrator Danych Osobowych.
4. Po otrzymaniu takiego powiadomienia Administrator Danych Osobowych podejmuje niezwłocznie czynności w celu ustalenia stanu faktycznego.
5. W przypadku uzasadnionego podejrzenia wystąpienia incydentu lub naruszenia systemu ochrony danych osobowych podejmuje działania mające zapobiec dalszym skutkom.
6. Po dokonaniu czynności zabezpieczających, Administrator Danych Osobowych, ma za zadanie przeprowadzić postępowanie wyjaśniające, które:
7. ustali ostateczny zakres, przyczyny wystąpienia oraz skutki, zarówno dla Praktyki, jak i osób, których dane dotyczyły,
8. podejmuje niezbędne czynności mające na celu przywrócenie prawidłowości działania systemu ochrony danych osobowych w podmiocie,
9. opracowuje działania naprawcze i zapobiegawcze, których zadaniem jest wyeliminowanie niepożądanych zdarzeń w przyszłości,
10. wskazuje osoby odpowiedzialne za wystąpienie sytuacji.
11. Powyższe czynności są dokumentowane przez Administratora Danych Osobowych za pomocą formularza, którego wzór stanowi załącznik nr 12.
12. Rejestr formularzy, o których mowa w punkcie 7 niniejszego rozdziału prowadzi Administrator lub wyznaczona przez administratora osoba..
13. Administrator powiadamia organ nadzorczy o incydencie lub naruszeniu systemu ochrony danych osobowych organ nadzorczynie później niż na 72 godziny od czasu jego wykrycia.

**§16**

**Kontrole wewnętrzne i audyty bezpieczeństwa**

1. Kontrolą przetwarzania danych osobowych zajmuje się Administrator Danych Osobowych.
2. Kontrole przeprowadzane są regularnie, co najmniej raz do roku, a w przypadku wystąpienia incydentu w podmiocie, kompleksową kontrolę obejmującą wszystkie aspekty działalności rozpoczyna się nie później niż 7 dni po zakończeniu działań związanych z incydentem, który wystąpił.
3. Kontrola przeprowadzana jest przy uwzględnieniu minimalnych wytycznych jakimi są: badanie pod względem zgodności z prawem, branżowymi standardami postepowania, normami i przepisami wewnętrznymi.
4. Administrator Danych Osobowych może wykonywać kontrole osobiście lub wyznaczyć do tego inną osobę lub podmiot.
5. Kontrole przeprowadzane są na podstawie programów kontroli, w których opisywany jest ich zakres, termin, cele oraz metody ich przeprowadzania oraz doraźnie.
6. Proces kontroli musi być dokumentowany i uzupełniony pozyskaniem obiektywnych dowodów na prawidłowość procesu kontrolnego.
7. Jeśli podczas kontroli stwierdzone zostają nieprawidłowości zagrażające systemowi ochrony danych osobowych w podmiocie, kontroler musi niezwłocznie powiadomić o tym fakcie administratora.
8. Wynik kontroli musi być udokumentowany i przekazany administratorowi w ciągu 21 dni od jej zakończenia.
9. Wzór raportu pokontrolnego określa załącznik nr 12.1.
10. Administrator może zlecić badanie audytowe niezależnemu podmiotowi.

**§17**

 **Środki techniczne ochrony danych osobowych**

**Ogólna ochrona budynku** – , monitoring wizyjny, całodobowy, gaśnice, systemy ppoż.

**Zabezpieczenia okien** – pomieszczenia zlokalizowane na parterze, okna zabezpieczone roletami materiałowymi oraz karatami zewnętrznymi.

**Zabezpieczenie drzwi** –drzwi tradycyjne zamykane na klucz.

**Zabezpieczenia zbiorów tradycyjnych (papierowych)** –do przechowywania danych stosuje się szafy tradycyjne oraz biurka zamykane na klucz. Dane przeznaczone do zniszczenia należy niszczyć w specjalistycznych niszczarkach.

**Zabezpieczenia zbiorów elektronicznych** – dane elektroniczne należy zabezpieczyć poprzez wyposażenie komputerów w zasilacze awaryjne podtrzymujące napięcie na wypadek braku zasilania oraz w systemy antywirusowe. Laptopy należy zabezpieczyć poprzez szyfrowanie dysku oraz ustawienie haseł dostępu. Telefony komórkowe oraz kartę pamięci należy zaszyfrować. Kopie danych z komputerów należy gromadzić w szafie/sejfie metalowym ognioodpornym*.*

Zabezpieczenie monitoringu wizyjnego – zapisy monitoringu wizyjnego przechowywane są 10 dni. Po tym czasie obraz z kamer