



**Młodzieżowy Ośrodek Socjoterapii**  
Dom Matki Dobrego Pasterza  
ul. Zgoda 14, 05-500 Piaseczno  
tel.: (22) 756-83-37; e-mail: poczta@mos-piaseczno.pl

## **POLITYKA OCHRONY DANYCH OSOBOWYCH**

### **W MŁODZIEŻOWYM OŚRODKU SOCJOTERAPII**

### **W PIASECZNIE**

Każda osoba ma prawo do ochrony jej życia prywatnego, rodzinnego, czci i dobrego imienia. Prawo do prywatności to jedno z podstawowych praw człowieka, a ochrona danych osobowych jest jednym z aspektów tego prawa.

Zadaniem niniejszego dokumentu, zwanego dalej Polityką, jest ustalenie wymogów, zasad i regulacji ochrony danych osobowych w Młodzieżowym Ośrodku Socjoterapii „Dom Matki Dobrego Pasterza” w Piasecznie, przy ul. Zgoda 14 .

Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu *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 (Dz.U.UE. L z dnia 4 maja 2016 r.); Dekretu ogólnego w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w Kościele katolickim wydanym przez Konferencję Episkopatu Polski w dniu 13 marca 2018 r. oraz odpowiednich przepisów prawa powszechnie obowiązującego.*

# ROZDZIAŁ I

## POSTANOWIENIA OGÓLNE

### **Art. 1. Przedmiot regulacji**

Niniejsza Polityka określa szczegółowe zasady ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w Młodzieżowym Ośrodku Socjoterapii w Piasecznie przy ul. Zgoda 14.

### **Art. 2. Zakres przedmiotowy**

Niniejsza Polityka ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych.

### **Art. 3. Zakres podmiotowy**

1. Niniejsza Polityka ma zastosowanie do Młodzieżowego Ośrodka Socjoterapii „Dom Matki Dobrego Pasterza” w Piasecznie przy ul. Zgoda 14, jako jednostki organizacyjnej powołanej przez Zgromadzenie Służebnic Matki Dobrego Pasterza, posiadające osobowość prawną na mocy art. 8 ust. 1 pkt. 6 ustawy z dn. 17.05.1989 r. o stosunku Państwa do Kościoła Katolickiego w RP (Dz. U. 2018.380 j.t.).
2. Za wdrożenie i utrzymanie Polityki odpowiada Dyrektor Młodzieżowego Ośrodka Socjoterapii.
3. Za stosowanie niniejszej Polityki odpowiedzialni są w szczególności Młodzieżowy Ośrodek Socjoterapii w Piasecznie, jego jednostki organizacyjne i wszyscy członkowie personelu.
4. Młodzieżowy Ośrodek Socjoterapii powinien zapewnić stosowanie tej Polityki z wszystkimi podmiotami współpracującymi na podstawie umów przetwarzania danych osobowych.

### **Art. 4. Słowniczek pojęć**

Na potrzeby niniejszej Polityki:

- 1) „dane osobowe” oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); 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;
- 2) „przetwarzanie” oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub

nieautomatyzowany, 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, niszczenie;

- 3) „zbiór danych” oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
- 4) „administrator” oznacza osobę prawną lub inną jednostkę organizacyjną, która ustala cele i sposoby przetwarzania danych osobowych;
- 5) „podmiot przetwarzający” oznacza osobę fizyczną lub prawną, bądź jednostkę organizacyjną, która przetwarza dane w imieniu administratora;
- 6) „odbiorca” oznacza osobę fizyczną lub prawną, organ publiczny, bądź jednostkę organizacyjną, której ujawnia się dane osobowe. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem, nie są jednak uznawane za odbiorców;
- 7) „zgoda” osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;
- 8) „naruszenie ochrony danych osobowych” oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
- 9) „dane wrażliwe” oznaczają dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne a także dane dotyczące zdrowia lub seksualności osoby fizycznej;
- 10) „dane genetyczne” oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;
- 11) „dane biometryczne” oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczny identyfikację tej osoby, takie jak np. wizerunek twarzy lub dane daktyloskopijne;
- 12) „dane dotyczące zdrowia” oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia.

## **ROZDZIAŁ II**

### **OCHRONA DANYCH OSOBOWYCH – ZASADY OGÓLNE**

#### **Art. 5. Filary ochrony danych osobowych w Młodzieżowym Ośrodku Socjoterapii:**

- (1) Legalność – Młodzieżowy Ośrodek Socjoterapii dba o ochronę prywatności i przetwarza dane zgodnie z prawem.
- (2) Bezpieczeństwo – Młodzieżowy Ośrodek Socjoterapii zapewnia odpowiedni poziom bezpieczeństwa danych podejmując stałe działania w tym zakresie.
- (3) Prawa Jednostki – Młodzieżowy Ośrodek Socjoterapii umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.
- (4) Rozliczalność – Młodzieżowy Ośrodek Socjoterapii dokumentuje to, w jaki sposób spełnia obowiązku, aby w każdej chwili móc wykazać zgodność.

#### **Art. 6. Zasady ochrony danych**

1. Młodzieżowy Ośrodek Socjoterapii w Piasecznie przetwarza dane osobowe z poszanowaniem następujących zasad:
  - 1) w oparciu o podstawę prawną i zgodnie z prawem (legalizm);
  - 2) rzetelnie i uczciwie (rzetelność);
  - 3) w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);
  - 4) w konkretnych celach i nie „na zapas” (minimalizacja);
  - 5) nie więcej niż potrzeba (adekwatność);
  - 6) z dbałością o prawidłowość danych (prawidłowość);
  - 7) nie dłużej niż potrzeba (czasowość);
  - 8) zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).
2. Za przestrzeganie określonych powyżej zasad odpowiedzialny jest administrator, który powinien być w stanie wykazać ich przestrzeganie. Na administratorze spoczywa obowiązek czuwania nad prawidłowym zachowaniem przedmiotowych norm kanonicznych oraz koordynacji działalności ewentualnych współpracowników.

#### **Art. 7. Dopuszczalność przetwarzania danych**

1. W działalności Młodzieżowego Ośrodka Socjoterapii przetwarzanie danych osobowych jest dopuszczalne, jeżeli:
  - 1) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
  - 2) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
  - 3) przetwarzanie jest niezbędne do wypełniania obowiązku prawnego ciążącego na administratorze, zgodnie z przepisami prawa powszechnie obowiązującego;

- 4) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
- 5) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- 6) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności, gdy osoba, której dane dotyczą, jest dzieckiem.

**Art. 8. Informowanie o przetwarzaniu danych w przypadku zbierania danych od osoby, której dane dotyczą**

1. W przypadku zbierania danych od osoby, której dane dotyczą, administrator danych informuje tę osobę o przetwarzaniu, podając informacje identyfikujące administratora i pozwalające się z nim skontaktować, bądź dane kontaktowe inspektora ochrony danych, wskazując cel przetwarzania danych, podstawę prawną przetwarzania, informacje o odbiorcach oraz zamiarze przekazania danych do innych osób prawnych mających siedzibę poza terytorium Rzeczypospolitej Polskiej. Ponadto administrator podaje informacje o okresie przetwarzania danych, informacje o prawie żądania od administratora dostępu do danych osobowych, prawie domagania się ich sprostowania, usunięcia lub ograniczenia przetwarzania zgodnie z niniejszą Polityką, oraz informacje o prawie wniesienia skargi do organu nadzorującego ochronę danych osobowych.
2. Przepis ust. 1 nie ma zastosowania w przypadku, gdy osoba, której dane dotyczą, dysponuje już tymi informacjami.

### **ROZDZIAŁ III**

#### **PRAWA OSOBY, KTÓREJ DANE DOTYCZĄ**

**Art. 9. Prawo do informacji o przetwarzaniu danych**

1. Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są jej dane osobowe, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz do otrzymania następujących informacji:
  - 1) cele przetwarzania;
  - 2) kategorie odnośnych danych osobowych;
  - 3) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione;
  - 4) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;

- 5) informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych, zgodnie z niniejszą Polityką;
  - 6) informacje o prawie wniesienia skargi do organu nadzorującego ochronę danych osobowych;
  - 7) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – informacje o ich źródle.
2. Administrator, ma obowiązek, na żądanie osoby, której dane dotyczą, dostarczyć jej kopię danych podlegających przetwarzaniu.

#### **Art. 10. Prawo do żądania sprostowania danych**

1. Osoba, której dane dotyczą, ma prawo żądać od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, jeżeli dane są nieprawidłowe.
2. Wniosek o sprostowanie danych powinien zostać przedstawiony w formie pisemnej administratorowi, osobiście lub za pośrednictwem prawnie ustanowionego pełnomocnika, z załączeniem właściwych dokumentów.
3. Jeżeli administrator odmówi przyjęcia wniosku o sprostowanie danych, powinien pisemnie powiadomić o odmowie wnioskodawcę, który będzie mógł złożyć ponownie wniosek do organu prowadzącego Młodzieżowy Ośrodek Socjoterapii w Piasecznie.

#### **Art.11. Prawo do żądania dokonania adnotacji i uzupełnienia danych**

1. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo w uzasadnionym zakresie żądać umieszczenia w zbiorze danych adnotacji lub uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.
2. Wniosek o dokonanie adnotacji lub uzupełnienie danych powinien spełniać warunki określone w art. 10 ust. 2.
3. Adnotacja dokonana na marginesie dokumentu stanowi jego część integralną. Jej treść winna być umieszczona w każdym wyciągu lub kopii aktu.
4. Administrator powiadamia pisemnie wnioskodawcę o dokonanej adnotacji.

#### **Art. 12. Prawo do żądania usunięcia danych**

1. Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:
  - 1) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
  - 2) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie danych, i nie ma innej podstawy prawnej przetwarzania;
  - 3) dane osobowe były przetwarzane niezgodnie z prawem.

2. Jeżeli administrator upublicznił dane osobowe, a ma obowiązek ich usunięcia, to – biorąc pod uwagę dostępną technologię i koszt realizacji – podejmuje rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych lub ich replikacje.
3. Zasady, o których mowa w ust. 1 i 2 nie mają zastosowania, w zakresie w jakim przetwarzanie jest niezbędne:
  - 1) do korzystania z prawa do swobody wypowiedzi i wolności informacji;
  - 2) do wywiązania się z obowiązku prawnego wymagającego przetwarzania lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
  - 3) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych albo do celów statystycznych, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania;
  - 4) do ustalenia, dochodzenia lub obrony roszczeń.

#### **Art. 13. Prawo do żądania ograniczenia przetwarzania**

1. Osoba, której dane dotyczą, ma prawo żądania od administratora ograniczenia przetwarzania danych w następujących przypadkach, gdy:
  - 1) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych;
  - 2) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystania;
  - 3) administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń.
2. Jeżeli na mocy ust. 1 przetwarzanie zostało ograniczone, takie dane osobowe można przetwarzać, z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego.
3. Przed uchyleniem ograniczenia przetwarzania administrator informuje o tym osobę, której dane dotyczą, która żądała ograniczenia na mocy ust. 1.

#### **Art. 14. Obowiązek powiadomienia**

1. Administrator informuje każdego odbiorcę, któremu ujawniono dane osobowe, o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.

Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

## ROZDZIAŁ IV

### ADMINISTRATOR I PODMIOT PRZETWARZAJĄCY

#### **Art. 15. Obowiązki administratora**

1. Administrator powinien wdrożyć odpowiednie środki techniczne i organizacyjne w celu ochrony danych, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych. Administrator jest zobowiązany do przestrzegania przepisów kanonicznych dotyczących starannego przechowywania, dozwolonego użytku i właściwego zarządzania danymi osobowymi.
2. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.
3. Zarówno na etapie projektowania, jak też w trakcie procesów przetwarzania administrator powinien zastosować odpowiednie środki techniczne i organizacyjne, służące ochronie danych a także pozwalające, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia celu przetwarzania.

#### **Art. 16. Współadministratorzy**

1. Jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, są oni współadministratorami. W drodze uzgodnień współadministratorzy w przejrzysty sposób określają odpowiednie zakresy swoich obowiązków i odpowiedzialności.
2. Uzgodnienia, o których mowa w ust. 1, należyście odzwierciedlają odpowiednie zakresy obowiązków współadministratorów oraz relacje pomiędzy nimi a podmiotami, których dane dotyczą. Zasadnicza treść uzgodnień jest udostępniana podmiotom, których dane dotyczą.
3. Niezależnie od uzgodnień, o których mowa w ust. 1, osoba, której dane dotyczą, może wykonywać przysługujące jej prawa wobec każdego z współadministratorów.

#### **Art. 17. Powierzenie przetwarzania i obowiązki podmiotu przetwarzającego**

1. Jeżeli przetwarzanie ma być dokonywane w imieniu administratora przez podmiot przetwarzający, podmiot ten powinien zapewniać wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszej Polityki i gwarantowało ochronę praw osób, których dane dotyczą.

2. Przetwarzanie danych przez podmiot przetwarzający powinno opierać się na umowie lub innym zobowiązaniu prawnym ustalającym zakres odpowiedzialności i procedury, gwarantującym, że podmiot przetwarzający:
  - 1) będzie przetwarzał dane wyłącznie w zakresie i celu określonym w umowie;
  - 2) zapewni, by osoby upoważnione do przetwarzania danych zobowiązały się do zachowania tajemnicy;
  - 3) podejmie środki wymagane w celu zabezpieczenia danych;
  - 4) będzie pomagał administratorowi wypełniać obowiązki w zakresie informowania osób, których dane dotyczą, realizowania ich uprawnień oraz obowiązki dotyczące zawiadamiania o naruszeniach;
  - 5) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usunie lub zwróci mu wszelkie dane osobowe oraz usunie wszelkie ich istniejące kopie;
  - 6) udostępni administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwi administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzenie audytów.
3. Podmiot przetwarzający nie może korzystać z usług innego podmiotu przetwarzającego bez uprzedniej pisemnej zgody administratora.

#### **Art. 18. Przetwarzanie z upoważnienia. Obowiązek zachowania tajemnicy.**

1. Podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenia administratora, chyba że wymaga tego prawo.
2. Administrator oraz każda inna osoba posiadająca stały dostęp do danych jest zobowiązana do zachowania tajemnicy dotyczącej wszystkich przetwarzanych danych osobowych. Obowiązek zachowania tajemnicy pozostaje nienaruszony także po zakończeniu pełnienia funkcji.

#### **Art. 19. Rejestrowanie czynności przetwarzania**

1. Każdy administrator prowadzi rejestr czynności przetwarzania danych osobowych, za które odpowiada. W rejestrze tym zamieszcza następujące informacje:
  - 1) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz współadministratorów, a także gdy ma to zastosowanie – inspektora ochrony danych;
  - 2) cele przetwarzania;
  - 3) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
  - 4) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione;
  - 5) gdy ma to zastosowanie, informacje o przekazywaniu danych do publicznej osoby prawnej mającej siedzibę poza terytorium Rzeczypospolitej Polskiej;

- 6) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
  - 7) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.
2. Każdy podmiot przetwarzający prowadzi rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora, zawierający następujące informacje:
- 1) imię i nazwisko lub nazwa oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający, a gdy ma to zastosowanie – inspektora ochrony danych;
  - 2) kategorie przetwarzania dokonywanych w imieniu każdego z administratorów;
  - 3) gdy ma to zastosowanie, informacje o przekazywaniu danych do publicznej osoby prawnej mającej siedzibę poza terytorium Rzeczypospolitej Polskiej;
  - 4) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.
3. Rejestry, o których mowa w ust. 1 i 2, mają formę pisemną, w tym elektroniczną.

#### **Art. 20. Bezpieczeństwo przetwarzania**

1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.
2. Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
3. Administrator oraz podmiot przetwarzający podejmują działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia administratora lub podmiotu przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie administratora, chyba że wymaga od niej prawo.

#### **Art. 21. Warunki przechowywania zbiorów danych**

1. Zbiory danych powinny być przechowywane w pomieszczeniu przeznaczonym do tego celu, bezpiecznym, należącym lub dostępnym wyłącznie dla administratora, podmiotu przetwarzającego oraz osób przetwarzających na podstawie upoważnienia.

2. W przypadku braku pomieszczenia o takich właściwościach, powinny być one przechowywane w szafie umieszczonej w lokalu należącym do administratora lub podmiotu przetwarzającego na zlecenie administratora lub dostępnym wyłącznie im i osobom przez nich upoważnionym, z wystarczającą gwarancją ich bezpieczeństwa i nienaruszalności.

#### **Art. 22. Przechowywanie danych w archiwach**

1. Szczególną uwagę należy zwrócić na zapewnienie nienaruszalności archiwów i ich zarządzanie.
2. Archiwum powinno być wyposażone w system zamknięcia, który gwarantuje wystarczającą ochronę przed kradzieżą i włamaniem.
3. Klucze do archiwum winny być starannie przechowywane przez administratora danych lub osobę przez niego upoważnioną. Staranność powinna być dochowana także przy autoryzacji dostępu udzielanego osobom postronnym.

#### **Art. 23. Przechowywanie danych w archiwach cyfrowych**

1. Dane zawarte w archiwach cyfrowych winny być zarządzane za pomocą licencjonowanego oprogramowania, pozwalającego na kontrolę dostępu przy pomocy systemu identyfikatorów i haseł dostępu.
2. Administrator winien zapewnić bezpieczeństwo danych poprzez okresowo dokonywany ich zapis i przeniesienie na inne nośniki, zabezpieczone przed dostępem osób postronnych.
3. Urządzenia i nośniki zawierające dane winny być przechowywane w pomieszczeniach zamkniętych i zabezpieczonych przed dostępem osób nieuprawnionych.

#### **Art. 24. Zgłaszanie naruszenia ochrony danych osobowych**

1. 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 organowi nadzorcemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
2. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi.
3. Zgłoszenie, o którym mowa w ust. 1, powinno co najmniej:
  - 1) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;

- 2) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenia innego punktu kontaktowego, od którego można uzyskać więcej informacji;
  - 3) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
  - 4) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
4. Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można ich udzielać sukcesywnie bez zbędnej zwłoki.
  5. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta powinna organowi nadzorczemu na weryfikowanie przestrzegania niniejszego artykułu.

#### **Art. 25. Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych**

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
2. Zawiadomienie, o którym mowa w ust. 1 niniejszego artykułu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art.24 ust. 3 pkt 2-4.
3. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:
  - 1) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
  - 2) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o których mowa w ust. 1;
  - 3) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

#### **Art. 26. Inspektor ochrony danych**

1. Administrator może wyznaczyć inspektora ochrony danych. W przypadku, gdy przetwarzanie danych odbywa się na dużą skalę, administrator powinien wyznaczyć inspektora ochrony danych.
2. Inspektor ochrony danych powinien być wyznaczony na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyki w dziedzinie ochrony danych oraz umiejętności wypełniania zadań, o których mowa w ust. 5.
3. Inspektor ochrony danych może być członkiem personelu administratora lub podmiotu przetwarzającego lub wykonywać zadania na podstawie umowy o świadczenie usług.
4. Osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszej Polityki.
5. Do zadań inspektora ochrony danych należy:
  - 1) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o spoczywających na nich obowiązkach w zakresie ochrony danych i doradzanie im w tej sprawie;
  - 2) monitorowanie przestrzegania niniejszej Polityki w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym autydy;
  - 3) współpraca z organem nadzorczym w ramach wykonywania przez niego zadań.
6. Administrator lub podmiot przetwarzający publikują dane kontaktowe inspektora ochrony danych i zawiadamiają o nich organ nadzorczy.

## **ROZDZIAŁ V**

### **ŚRODKI OCHRONY PRAWNEJ**

#### **Art. 27. Procedura odwoławcza**

Jeżeli osoba, której dane dotyczą, uzna, że przetwarzanie danych nie jest zgodne z przepisami niniejszej Polityki, może złożyć skargę do organu nadzorczego.

#### **ZALĄCZNIKI:**

1. Oświadczenie pracownika o zachowaniu poufności i zapoznaniu się z przepisami
2. Rejestr realizacji żądań podmiotu danych
3. Upoważnienie do przetwarzania danych osobowych
4. Odwołanie upoważnienia do przetwarzania danych osobowych
5. Rejestr osób upoważnionych do przetwarzania danych
6. Raport z naruszenia bezpieczeństwa danych

7. Instrukcja zarządzania systemem informatycznym i procedury postępowania
8. Polityka czystego biurka
9. Instrukcja w sprawie określenia procedury postępowania z kluczami oraz zabezpieczenia pomieszczeń
10. Rejestr czynności przetwarzania danych osobowych