POLITYKA OCHRONY DANYCH OSOBOWYCH

POLSKIEGO STOWARZYSZENIA NA RZECZ OSÓB Z NIEPEŁNOSPRAWNOŚCIĄ INTELEKTUALNĄ

KOŁO W NOWYM TARGU

SPIS TREŚCI

TYTUŁ I.
SKRÓTY I DEFINICJE

Na użytek niniejszej Polityki ochrony danych osobowych:

1) „**Administrator Danych (zwany też Administrator)**” – oznacza PSONI Koło w Nowym Targu, ul. Podtatrzańska 47a, 34-400 Nowy Targ, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;
2) **„Placówka”** – oznacza:

a) Środowiskowy Dom Samopomocy w Nowym Targu przy ulicy
b) Szkoła Przysposabiająca do Pracy w Nowym Targu przy ulicy
c) Ośrodek Rehabilitacyjno-Edukacyjno-Wychowawczy w Nowym Targu przy ulicy
d) Zespół Wczesnego Wspomagania Rozwoju w Nowym Targu przy ulicy
e) Specjalistyczna Placówka Rehabilitacji i Wsparcia w Nowym Targu przy ulicy
- prowadzone przez PSONI Koło w Nowym Targu.;

3) **„Polityka”** - oznacza niniejszą Politykę ochrony danych osobowych, o ile co innego nie wynika wyraźnie z kontekstu;
4) **Instrukcja** – oznacza Instrukcję Zarządzania Systemem Informatycznym w PSONI Koło w Nowym Targu ;
5) „**RODO”** - oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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 119, s. 1);
6) „**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;
7) **„dane szczególnych kategorii”** - oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej;
8) **„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;
9) **„dane biometryczne”** - oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną

identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;

10) **„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;
11) **„dane karne”** - oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa;
12) **„dane dzieci”** - oznaczają dane osób poniżej 16 roku życia;
13) **„zbiór danych”** oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
14) **„osoba”** - oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu;
15) „**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;
16) **„ograniczenie przetwarzania”** oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
17) **„profilowanie”** oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
18) **„pseudonimizacja”** oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
19) **„podmiot przetwarzający”**- oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
20) **„odbiorca”** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;
21) **„strona trzecia”** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;

22) **„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;
23) **„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;
24) **„organ nadzorczy”** - oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51 RODO;
25) **„transgraniczne przetwarzanie”** - oznacza:
przetwarzanie danych osobowych, które odbywa się w Unii w ramach działalności jednostek organizacyjnych w więcej, niż jednym państwie członkowskim administratora lub podmiotu przetwarzającego w Unii posiadającego jednostki organizacyjne w więcej niż jednym państwie członkowskim; albo
przetwarzanie danych osobowych, które odbywa się w Unii w ramach działalności pojedynczej jednostki organizacyjnej administratora lub podmiotu przetwarzającego w Unii, ale które znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, w więcej niż jednym państwie członkowskim;
26) **„eksport danych”** - oznacza przekazanie danych do państwa trzeciego (czyli poza UE, Norwegię, Liechtenstein, Islandię) lub organizacji międzynarodowej;
27) **„organizacja międzynarodowa”** - oznacza organizację i organy jej podlegające działające na podstawie prawa międzynarodowego publicznego lub inny organ powołany w drodze umowy między co najmniej dwoma państwami lub na podstawie takiej umowy;
28) „**IOD” lub „Inspektor”** - oznacza Inspektora Ochrony Danych Osobowych;
29) **„RCPD” lub „Rejestr”** oznacza Rejestr Czynności Przetwarzania Danych Osobowych;
30) **„System informatyczny”** – oznacza zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji narzędzi programowych zastosowanych w celu przetwarzania danych;
31) **„użytkownik”** – oznacza osobę upoważnioną przez Administratora Danych do Przetwarzania danych osobowych;
32) **„identyfikator użytkownika”** – oznacza ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w takim systemie;
33) **„hasło”** – oznacza ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym (Użytkownikowi) w razie przetwarzania danych osobowych w takim systemie;
34) **„uwierzytelnianie”** – oznacza działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu (Użytkownika);
35) **ASI –** Administrator Systemu Informatycznego**.**

TYTUŁ II.
PODSTAWOWE INFORMACJE

DZIAŁ I.
POSTANOWIENIA OGÓLNE

1. Niniejszy dokument zatytułowany „Polityka ochrony danych osobowych” (**dalej: Polityka)** określa zasady i tryb postępowania przy przetwarzaniu danych osobowych w PSONI Koło w Nowym Targu, ul. Podtatrzańska 47a, 34-400 Nowy Targ.
2. Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO – rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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 119, s. 1).
3. Celem Polityki jest zapewnienie ochrony i bezpieczeństwa danych osobowych przetwarzanych w PSONI Koło w Nowym Targu, ul. Podtatrzańska 47a, 34-400 Nowy Targ, zgodnie z wymogami RODO oraz ustawodawstwa krajowego.
4. Polityka wyraża wolę Administratora w zakresie ochrony jej zasobów informacyjnych oraz zasobów służących do przetwarzania informacji.
5. Administrator aktywnie wspiera procesy zmierzające do zapewnienia bezpieczeństwa informacji poprzez wdrażanie, rozwój i uaktualnianie Polityki oraz wynikających z niej regulacji.
6. Odpowiedzialny za wdrożenie, utrzymanie, nadzór i monitorowanie przestrzegania, niniejszej Polityki jest Zarząd Stowarzyszenia.
7. Za stosowanie niniejszej Polityki odpowiedzialni są:
) Administrator;
) wszyscy członkowie personelu Administratora oraz współpracownicy Stowarzyszenia.
8. Administrator powinien też zapewnić zgodność postępowania jego kontrahentów z niniejszą Polityką w odpowiednim zakresie, gdy dochodzi do przekazania im danych osobowych przez Administratora
9. Polityka jest przechowywana w wersji elektronicznej oraz w wersji papierowej w siedzibie Administratora.

DZIAŁ II.
OBSZAR PRZETWARZANIA DANYCH

Określenie obszaru, w którym przetwarzane są dane osobowe obejmuje:

1) miejsca, w których wykonuje się operacje na danych osobowych (wpisuje, modyfikuje, kopiuje);
2) miejsca, gdzie przechowuje się wszelkie nośniki informacji zawierające dane osobowe

(szafy z dokumentacją papierową, szafy zawierające komputerowe nośniki informacji z kopiami zapasowymi danych, stacje komputerowe, serwery i inne urządzenia komputerowe, jak np. macierze dyskowe, na których dane osobowe są przetwarzane na bieżąco).

DZIAŁ III.
DANE OSOBOWE, WYKAZ ZBIORÓW, OPIS STRUKTURY I SPOSÓB PRZEPŁYWU

1. Administrator przetwarza dane osobowe zwykłe (art. 6 ust.1 RODO), szczególne kategorie danych osobowych (art. 9 ust. 2 RODO).
2. Administrator nie podejmuje czynności przetwarzania, które mogłyby wiązać się z poważnym prawdopodobieństwem wystąpienia wysokiego ryzyka dla praw i wolności osób. W przypadku planowania takiego działania Administrator wykona czynności określone w art. 35 i nast. RODO.
3. W przypadku planowania nowych czynności przetwarzania Administrator dokonuje analizy ryzyka związanego z przetwarzaniem danych osobowych oraz uwzględnia kwestie ochrony danych osobowych w fazie ich projektowania.
4. Polityka dotyczy wszystkich danych przetwarzanych przez Administratora niezależnie od formy ich przetwarzania (przetwarzanie zautomatyzowane i niezautomatyzowane) oraz od tego, czy dane są lub mogą być przetwarzane w zbiorach danych.

TYTUŁ III.
OCHRONA DANYCH OSOBOWYCH W HOTELU

DZIAŁ I .
POSTANOWIENIA OGÓLNE

1. Filary ochrony danych osobowych w Hotelu:
   -) **Legalność** – Administrator dba o ochronę prywatności i przetwarza dane zgodnie z prawem;
   -) **Bezpieczeństwo** – Administrator zapewnia odpowiedni poziom bezpieczeństwa danych, podejmując stale działania w tym zakresie;
   -) **Prawa jednostki** – Administrator umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje;
   -) **Rozliczalność** – Administrator dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.
2. System ochrony danych osobowych składa się z następujących elementów:
   -) **Inwentaryzacja danych** - Administrator dokonuje identyfikacji przetwarzanych przez niego zasobów danych osobowych, kategorii/rodzajów danych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych, w tym:
     -) przypadków przetwarzania danych szczególnych kategorii;
     -) przypadków przetwarzania danych osób, których Administrator nie

identyfikuje (dane niezidentyfikowane);
-) przypadków przetwarzania danych dzieci;
-) profilowania;
-) współadministrowania danymi.

) **Rejestr** - Administrator opracowuje, prowadzi i utrzymuje Rejestr. Rejestr jest narzędziem rozliczania zgodności z ochroną danych w Hotelu;

) **Podstawy prawne przetwarzania** - Administrator zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze, w tym:
-) utrzymuje system zarządzania zgodami na przetwarzanie danych i komunikację na odległość;
-) inwentaryzuje i uszczegóławia uzasadnienie przypadków, gdy Administrator przetwarza dane na podstawie prawnie uzasadnionego interesu Administratora.

4) **Obsługa praw jednostki** – Administrator spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:
-) obowiązki informacyjne - Administrator przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków;
-) możliwość wykonania żądań - Administrator weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania osoby przez siebie i swoich przetwarzających;
-) obsługa żądań - Administrator zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany przez RODO i dokumentowane;
-) zawiadamianie o naruszeniach - Administrator stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.

5) **Minimalizacja** – Administrator posiada zasady i metody zarządzania minimalizacją (privacy by default), a w tym:
-) zasady zarządzania adekwatnością danych;
-) zasady reglamentacji i zarządzania dostępem do danych;
-) zasady zarządzania okresem przechowywania danych i weryfikacji dalszej przydatności.

6) **Bezpieczeństwo** - Administrator zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:
-) przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii;
-) przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie;
-) dostosowuje środki ochrony danych do ustalonego ryzyka;
-) posiada system zarządzania bezpieczeństwem informacji;
-) stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Organowi Nadzoru– zarządza incydentami.

7) **Przetwarzający** - Administrator posiada zasady doboru przetwarzających dane na rzecz Administratora, wymogów co do warunków przetwarzania (umowa

powierzenia), zasad weryfikacji wykonywania umów powierzenia;

8) **Eksport danych** - Administrator posiada zasady weryfikacji, czy Administrator nie przekazuje danych do państw trzecich (czyli poza UE, Norwegię, Liechtenstein, Islandię) lub do organizacji międzynarodowych oraz zapewnienia zgodne z prawem warunki takiego przekazywania, jeśli ma ono miejsce;
9) **Privacy by design** - Administrator zarządza zmianami wpływającymi na prywatność. W tym celu procedury uruchamiania nowych projektów i inwestycji w Hotelu uwzględniają konieczność oceny wpływu zmiany na ochronę danych, analizę ryzyka, zapewnienie prywatności (a w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu;
10) **Przetwarzanie transgraniczne** - Administrator weryfikuje, kiedy zachodzą przypadki przetwarzania transgranicznego.

DZIAŁ II.
INWENTARYZACJA DANYCH

1. Administrator przetwarza dane osobowe z poszanowaniem następujących podstawowych zasad wskazanych w art. 5 RODO:
) **„zasady zgodności z prawem, rzetelności i przejrzystości”** – dane osobowe przetwarzane są zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą. Dla osób fizycznych powinno być przejrzyste, że dotyczące ich dane osobowe są zbierane, wykorzystywane, przeglądane lub w inny sposób przetwarzane oraz w jakim stopniu te dane osobowe są lub będą przetwarzane. Zasada przejrzystości wymaga, by wszelkie informacje i wszelkie komunikaty związane z przetwarzaniem tych danych osobowych były łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem. Zasada ta dotyczy w szczególności informowania osób, których dane dotyczą, o tożsamości administratora i celach przetwarzania oraz innych informacji mających zapewnić rzetelność i przejrzystość przetwarzania w stosunku do osób, których sprawa dotyczy, a także prawa takich osób do uzyskania potwierdzenia i informacji o przetwarzanych danych osobowych ich dotyczących. Osobom fizycznym należy uświadomić ryzyka, zasady, zabezpieczenia i prawa związane z przetwarzaniem danych osobowych oraz sposoby wykonywania praw przysługujących im w związku z takim przetwarzaniem;
) „**zasady ograniczenia celu”** – dane osobowe zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami, chyba że:
) dalsze przetwarzanie odbywa się na podstawie przepisów prawa unijnego lub krajowego;
) Administrator uzyskał zgodę na osoby, której dane dotyczą na dalsze przetwarzanie;
) wtórny cel przetwarzania nie jest niezgodny z celem pierwotnym;
) „**zasady minimalizacji danych”** – dane osobowe są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;
) „**zasady prawidłowości danych”** – dane osobowe są 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;

) **„zasady ograniczenia przechowywania”** – dane osobowe są 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; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 RODO, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą;

) „**zasady integralności i poufności”** - dane osobowe są 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;

) **„zasady rozliczalności”** - Administrator jest odpowiedzialny za przestrzeganie zasad z pkt 1- 6 i musi być w stanie wykazać ich przestrzeganie;

2. Przetwarzanie **<u>danych osobowych zwykłych</u>** jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków **(podstawy prawne przetwarzania danych osobowych zwykłych):**

) osoba, której dane dotyczą wyraziła **zgodę** na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów **(art. 6 ust. 1 lit. a RODO):**

) administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych;

) jeżeli osoba, której dane dotyczą, wyrażą zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem i nie powinno zawierać nieuczciwych warunków. W szczególności w przypadku pisemnego oświadczenia składanego w innej sprawie powinny istnieć gwarancje, że osoba, której dane dotyczą, jest świadoma wyrażenia zgody oraz jej zakresu. Część takiego oświadczenia osoby, której dane dotyczą, stanowiąca naruszenie RODO nie jest wiążąca. Aby wyrażenie zgody było świadome, osoba, której dane dotyczą, powinna znać przynajmniej tożsamość administratora oraz zamierzone cele przetwarzania danych osobowych;

c) osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie;

d) oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy między innymi od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie

danych osobowych nie jest niezbędne do wykonania tej umowy. Aby zapewnić dobrowolność, zgoda nie powinna stanowić ważnej podstawy prawnej przetwarzania danych osobowych w szczególnej sytuacji, w której istnieje wyraźny brak równowagi między osobą, której dane dotyczą, a administratorem. Wyrażenia zgody nie należy uznawać za dobrowolne, jeżeli osoba, której dane dotyczą, nie ma rzeczywistego lub wolnego wyboru oraz nie może odmówić ani wycofać zgody bez niekorzystnych konsekwencji. Zgody nie uważa się za dobrowolną, jeżeli nie można jej wyrazić z osobna na różne operacje przetwarzania danych osobowych, mimo że w danym przypadku byłoby to stosowne, lub jeżeli od zgody uzależnione jest wykonanie umowy – w tym świadczenie usługi – mimo że do jej wykonania zgoda nie jest niezbędna;

e) zgoda powinna być wyrażona w drodze jednoznacznej, potwierdzającej czynności, która wyraża odnoszące się do określonej sytuacji dobrowolne, świadome i jednoznaczne przyzwolenie osoby, których dane dotyczą, na przetwarzanie dotyczących jej danych osobowych i która ma na przykład formę pisemnego (w tym elektronicznego) lub ustnego oświadczenia. Może to polegać na zaznaczeniu okienka wyboru podczas przeglądania strony internetowej, na wyborze ustawień technicznych do korzystania z usług społeczeństwa informacyjnego lub też na innym oświadczeniu bądź zachowaniu, które w danym kontekście jasno wskazuje, że osoba, której dane dotyczą, zaakceptowała proponowane przetwarzanie jej danych osobowych. Milczenie, okienka domyślnie zaznaczone lub niepodjęcie działania nie powinny zatem oznaczać zgody. Zgoda powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach. Jeżeli przetwarzanie służy różnym celom, potrzebna jest zgoda na wszystkie te cele. Jeżeli osoba, której dane dotyczą, ma wyrazić zgodę w odpowiedzi na elektroniczne zapytanie, zapytanie takie musi być jasne, zwięzłe i nie zakłócać niepotrzebnie korzystania z usługi, której dotyczy.

) 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 **(art. 6 ust. 1 lit. b RODO)**;

) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze **(art. 6 ust. 1 lit. c RODO);**

) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej **(art. 6 ust. 1 lit. d RODO);**

) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi **(art. 6 ust. 1 lit. e RODO);**

) 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. 6 ust. 1 lit. f RODO).**

3. Przetwarzanie **danych osobowych szczególnej kategorii** jest zgodne z prawem wyłącznie w

przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków **(podstawy prawne przetwarzania danych osobowych szczególnej kategorii):**

) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba
że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu przetwarzania danych osobowych szczególnej kategorii (**art. 9 ust. 2 lit. a RODO**) – co do warunków zgody patrz ust. 2 pkt 1 lit a-e;

) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą (**art. 9 ust. 2 lit. b RODO**);

3) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody (**art. 9 ust. 2 lit c RODO**);
4) przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą (**art. 9 ust. 2 lit. d RODO**);
5) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą (**art. 9 ust. 2 lit. e RODO**);
6) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy (**art. 9 ust. 2 lit. f RODO**);
7) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą (**art. 9 ust. 2 lit. g RODO**);
8) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń (**art. 9 ust. 2 lit. h RODO**). Dane mogą być przetwarzane do tego celu jeżeli są przetwarzane przez - lub na odpowiedzialność - pracownika podlegającego obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe lub przez inną osobę również podlegającą obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub

prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe;

9) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową (**art. 9 ust. 2 lit. i RODO**);

) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 RODO, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą (**art. 9 ust. 2 lit. j RODO**);

4. Ponieważ co do zasady zgodnie z art. 9 ust. 1 RODO przetwarzanie danych osobowych szczególnej kategorii jest zakazane, Administrator identyfikuje przypadki, w których przetwarza lub może przetwarzać dane szczególnych kategorii oraz utrzymuje dedykowane mechanizmy zapewnienia zgodności z prawem przetwarzania takich danych.
5. Administrator identyfikuje przypadki, w których przetwarza lub może przetwarzać dane niezidentyfikowane i utrzymuje mechanizmy ułatwiające realizację praw osób, których dotyczą dane niezidentyfikowane.
6. Administrator identyfikuje przypadki, w których dokonuje profilowania przetwarzanych danych, i utrzymuje mechanizmy zapewniające zgodność tego procesu z prawem.
7. Administrator identyfikuje przypadki współadministrowania danymi.

DZIAŁ III.
REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH
(ART. 30 RODO)

1. Rejestr stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.
2. Administrator prowadzi Rejestr, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.
3. Rejestr jest jednym z podstawowych narzędzi umożliwiających Administratorowi rozliczanie większości obowiązków ochrony danych.
4. W Rejestrze dla każdej czynności przetwarzania danych, którą Administrator uznał za odrębną dla potrzeb Rejestru, odnotowuje co najmniej:

) nazwę czynności;

) cel przetwarzania;

3) opis kategorii osób, których dane dotyczą;
4) opis kategorii danych osobowych;
5) podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego

interesu Administratora, jeśli podstawą jest uzasadniony interes;
6) sposób zbierania danych;
7) opis kategorii odbiorców, którym dane osobowe zostały lub zostaną ujawnione (w tym przetwarzających);
8) informację o przekazaniu poza EU/EOG;
9) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
10) ogólny opis technicznych i organizacyjnych środków ochrony danych.

DZIAŁ IV.
PODSTAWY PRAWNE PRZETWARZANIA

1. Administrator dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.
2. Wskazując w dokumentach ogólną podstawę prawną RODO Administrator dookreśla podstawę w precyzyjny i czytelny sposób, gdy jest to potrzebne.
3. Administrator wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikację na odległość (e-mail, telefon, SMS itp.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności(sprzeciw, ograniczenie itp.).
4. Kierownik komórki organizacyjnej Administratora ma obowiązek znać podstawy prawne, na jakich komórka przez niego kierowana dokonuje konkretnych czynności przetwarzania danych osobowych. Jeżeli podstawą jest uzasadniony interes Administratora, kierownik komórki ma obowiązek znać konkretny realizowany przetwarzaniem interes Administratora.

DZIAŁ V.
OBSŁUGA PRAW JEDNOSTKI

ROZDZIAŁ I .
POSTANOWIENIA OGÓLNE

ODDZIAŁ I.
POSTANOWIENIA OGÓLNE

Administrator określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.

ODDZIAŁ II.
DANE OSOBOWE POZYSKANE OD OSOBY, KTÓREJ DANE DOTYCZĄ (ART. 13 RODO)

1. **Jeżeli dane osobowe pozyskano od osoby, której dane dotyczą**, Administrator podczas pozyskiwania danych osobowych podaje jej wszystkie następujące informacje:
) swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;

) gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych;
) cele przetwarzania, do których mają posłużyć dane osobowe, oraz podstawę prawną przetwarzania;
) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
) gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46 RODO, art. 47 RODO lub art. 49 ust. 1 akapit drugi RODO, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.

2. Poza informacjami, o których mowa w pkt 1, Administrator podaje osobie, której dane dotyczą, następujące informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania wobec tej osoby:
) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) RODO– prawnie uzasadnione interesy realizowane przez Administratora lub przez stronę trzecią;
) 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;
) 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;
) informacje o prawie wniesienia skargi do organu nadzorczego;
) źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych;
) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

3. Jeżeli Administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym te dane zostały pozyskane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w pkt. 2
4. Punkty 1-3 nie mają zastosowania, gdy – i w zakresie - w jakim osoba, której dane dotyczą, dysponuje już tymi informacjami.

ODDZIAŁ III.
DANE OSOBOWE NIE POZYSKANE OD OSOBY, KTÓREJ DANE DOTYCZĄ (ART. 14 RODO)

1. Jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą, Administrator podaje

osobie, której dane dotyczą, następujące informacje:

) swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;
) gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych;
) cele przetwarzania, do których mają posłużyć dane osobowe, oraz podstawę prawną przetwarzania;
) kategorie odnośnych danych osobowych;
) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
) gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46 RODO, art. 47 RODO lub art. 49 ust. 1 akapit drugi RODO , wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.

2. Poza informacjami, o których mowa w pkt. 1, Administrator podaje osobie, której dane dotyczą, następujące informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania wobec osoby, której dane dotyczą:

) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) RODO– prawnie uzasadnione interesy realizowane przez Administratora lub przez stronę trzecią;
) 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;
) 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;
) informacje o prawie wniesienia skargi do organu nadzorczego;
) źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych;
) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

3. Informacje, o których mowa w pkt. 1-2, Administrator podaje:

) w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca – mając na uwadze konkretne okoliczności przetwarzania danych osobowych;
) jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą; lub
) jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich

pierwszym ujawnieniu.

4. Jeżeli Administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym te dane zostały pozyskane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w pkt. 2.
5. Punkty 1-4 nie mają zastosowania, gdy – i w zakresie, w jakim:
) osoba, której dane dotyczą, dysponuje już tymi informacjami;
) udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku; w szczególności w przypadku przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem warunków i zabezpieczeń, o których mowa w art. 89 ust. 1 RODO, lub o ile obowiązek, o którym mowa w pkt. 1 , może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania. W takich przypadkach Administrator podejmuje odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osoby, której dane dotyczą, w tym udostępnia informacje publicznie;
   3) pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą
   4) dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy.

ODDZIAŁ IV.
INNE OBOWIĄZKI INFORMACYJNE

1. Administrator określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam, gdzie to jest możliwe.
2. Administrator przed uchyleniem ograniczenia przetwarzania informuje o tym osobę, której dane dotyczą, która żądała ograniczenia.
3. Administrator informuje o sprostowaniu/uzupełnieniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, których dokonał zgodnie z art. 16, art. 17 ust. 1 i art. 18 RODO, każdego odbiorcę, któremu ujawniono dane osobowe, 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.
4. Administrator najpóźniej przy okazji pierwszej komunikacji z osobą, której dane dotyczą, wyraźnie informuje ją o prawie wniesienia sprzeciwu wobec przetwarzania jej danych osobowych oraz przedstawia się je jasno i odrębnie od wszelkich innych informacji.
5. Administrator bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

ROZDZIAŁ II .
OBSŁUGA ŻĄDAŃ OSÓB

ODDZIAŁ I.
PRAWO DOSTĘPU DO DANYCH
(ART. 15 RODO)

Prawo dostępu przysługujące osobie, której dane dotyczą:

1) Osoba, której dane dotyczą, jest uprawniona do uzyskania od Administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:
) cele przetwarzania;
) kategorie odnośnych danych osobowych;
) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
) informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
) informacje o prawie wniesienia skargi do organu nadzorczego;
) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;
) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.
2) Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach, o których mowa w art. 46 RODO, związanych z przekazaniem.
3) Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, Administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną. Kopii danych wydanej w wykonaniu prawa dostępu do danych Administrator nie uzna za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych.
4) Na żądanie osoby, której dane dotyczą Administrator wydaje kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych.

ODDZIAŁ II.
PRAWO DO SPROSTOWANIA DANYCH
(ART. 16 RODO)

1. Osoba, której dane dotyczą, ma prawo żądania od Administratora niezwłocznego

sprostowania dotyczących jej danych osobowych, które są nieprawidłowe.
2. Administrator ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga.
3. W przypadku sprostowania danych Administrator informuje osobę o odbiorcach danych, na żądanie tej osoby.

ODDZIAŁ III.
PRAWO DO UZUPEŁNIENIA DANYCH
(ART. 16 RODO)

1. Z uwzględnieniem celów przetwarzania danych osobowych, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.
2. Administrator ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych (np. Administrator nie musi przetwarzać danych, które są zbędne).
3. Administrator może polegać na oświadczeniu osoby co do uzupełnianych danych, chyba że będzie to niewystarczające lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.

ODDZIAŁ IV.
PRAWO DO USUNIĘCIA DANYCH
„PRAWO DO BYCIA ZAPOMNIANYM”
(ART. 17 RODO)

1. Osoba, której dane dotyczą, ma prawo żądania od Administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a Administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:
) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie zgodnie z art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a RODO i nie ma innej podstawy prawnej przetwarzania;
) osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 RODO wobec przetwarzania;
) dane osobowe były przetwarzane niezgodnie z prawem;
) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator;
) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku;
2. Jeżeli Administrator upublicznił dane osobowe, a na skutek zgłoszenia żądania do usunięcia danych ma obowiązek usunąć te dane osobowe, 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 osobowych lub ich replikacje.

3. Administrator określa sposób obsługi prawa do usunięcia danych w taki sposób, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony danych, w tym bezpieczeństwa, a także weryfikację, czy nie zachodzą wyjątki, o których mowa w art. 17. ust. 3 RODO, zgodnie z którymi punkty 1 i 2 nie mają zastosowania, w zakresie w jakim przetwarzanie jest niezbędne:
) do korzystania z prawa do wolności wypowiedzi i informacji;
) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
) z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h) oraz i) i art. 9 ust. 3 RODO;
) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 RODO, o ile prawdopodobne jest, że prawo do usunięcia danych, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania;
) do ustalenia, dochodzenia lub obrony roszczeń;
   6) W przypadku usunięcia danych Administrator informuje osobę o odbiorcach danych, na żądanie tej osoby.

ODDZIAŁ V.
PRAWO DO OGRANICZENIA PRZETWARZANIA DANYCH
(ART. 18 RODO)

1. Osoba, której dane dotyczą, ma prawo żądania od Administratora ograniczenia przetwarzania w następujących przypadkach:
) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych;
) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
) Administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
) osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.
2. W trakcie ograniczenia przetwarzania Administrator co do zasady tylko przechowuje dane osobowe. Może je przetwarzać tylko w następujących sytuacjach:
) wyłącznie za zgodą osoby, której dane dotyczą;
) w celu ustalenia, dochodzenia lub obrony roszczeń;
) w celu ochrony praw innej osoby fizycznej lub prawnej;
) z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.
3. Przed uchyleniem ograniczenia przetwarzania administrator informuje o tym osobę, której

dane dotyczą, która żądała ograniczenia.

4. W przypadku ograniczenia przetwarzania danych Administrator informuje osobę o odbiorcach danych, na żądanie tej osoby.

ODDZIAŁ VI.
PRAWO DO PRZENOSZENIA DANYCH
(ART. 20 RODO)

Na żądanie osoby Administrator wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, jeśli jest to możliwe, dane dotyczące tej osoby, które dostarczyła ona Administratorowi, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej w systemach informatycznych Administratora.

ODDZIAŁ VII.
PRAWO DO SPRZECIWU
(ART. 21 RODO)

1. Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez Administratora w oparciu o:
) uzasadniony interes Administratora;
) powierzone Administratorowi zadanie w interesie publicznym.
2. Administrator uwzględni sprzeciw, o ile nie zachodzą po stronie Administratora:
) ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw;
) podstawy do ustalenia, dochodzenia lub obrony roszczeń.
3. Jeżeli Administrator przetwarza dane w celach statystycznych, osoba może wnieść umotywowany jej szczególną sytuacją sprzeciw względem takiego przetwarzania. Administrator uwzględni taki sprzeciw, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.
4. Jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez Administratora na potrzeby marketingu bezpośredniego (w tym ewentualnie profilowania), Administrator uwzględni sprzeciw i zaprzestanie takiego przetwarzania.
5. Administrator najpóźniej przy okazji pierwszej komunikacji z osobą, której dane dotyczą, wyraźnie informuje ją o prawie wniesienia sprzeciwu wobec przetwarzania jej danych osobowych, oraz przedstawia się je jasno i odrębnie od wszelkich innych informacji.
6. W związku z korzystaniem z usług społeczeństwa informacyjnego i bez uszczerbku dla dyrektywy 2002/58/WE osoba, której dane dotyczą, może wykonać prawo do sprzeciwu za pośrednictwem zautomatyzowanych środków wykorzystujących specyfikacje techniczne.

ROZDZIAŁ III.
ZAWIADOMIENIA O NARUSZENIACH

1. W przypadku stwierdzenia naruszenia ochrony Danych osobowych Administrator

dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych. Jeżeli ryzyko naruszenia praw i wolności jest wysokie, Administrator zawiadamia o incydencie także osobę, której dane dotyczą.

2. Za naruszenie bezpieczeństwa danych osobowych należy uznać wszelkie zdarzenia lub działania, które mogą prowadzić do utraty danych osobowych, naruszenia poufności, integralności lub dostępności danych osobowych, naruszenia niezawodności systemów służących do przetwarzania danych osobowych.
3. Każdy pracownik i współpracownik Administratora, który stwierdzi fakt naruszenia bezpieczeństwa danych osobowych, bądź posiada informację mogącą mieć wpływ na bezpieczeństwo danych osobowych jest zobowiązana niezwłocznie zgłosić to Administratorowi, ASI lub bezpośredniemu przełożonemu.
4. Ponadto każdy pracownik i współpracownik Administratora ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenia danych osobowych oraz w miarę możliwości ustalić przyczynę i sprawcę naruszenia danych osobowych.
5. Administrator, ASI lub powołany przez Administratora IOD dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych osobowych oraz czynności jakie zostały podjęte po stwierdzeniu naruszenia danych i sporządza raport oraz przekazuje go Administratorowi.
6. W zależności od przyczyny naruszenia zabezpieczeń ochrony danych osobowych (technicznych, organizacyjnych lub celowych) podejmowane są odpowiednie działania zmierzające w przyszłości do uniknięcia ich wystąpienia.
7. Administrator podejmuje odpowiednie działania w stosunku do osób, które naruszyły zasady ochrony danych osobowych oraz w razie potrzeby składa do organów ścigania zawiadomienie o podejrzeniu popełnienia przestępstwa.
8. W każdej sytuacji, w której zaistniałe naruszenia mogły spowodować ryzyko naruszenia praw lub wolności osób fizycznych, Administrator zgłasza ten fakt organowi nadzorczemu bez zbędnej zwłoki – jeżeli to wykonalne, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia.
9. Administrator prowadzi ewidencję naruszeń ochrony danych.

DZIAŁ VI.
MINIMALIZACJA

ROZDZIAŁ I.
POSTANOWIENIA OGÓLNE

Administrator dba o minimalizację przetwarzania danych pod kątem:

1) adekwatności danych do celów (ilości danych i zakresu przetwarzania);
2) dostępu do danych;
3) czasu przechowywania danych.

ROZDZIAŁ II.
MINIMALIZACJA ZAKRESU

1. Administrator weryfikuje zakres pozyskiwanych danych, zakres ich przetwarzania i ilość

przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO.

2. Administrator dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok. Administrator przeprowadza weryfikację zmian co do ilości i zakresu przetwarzania danych w ramach procedur zarządzania zmianą **(privacy by design).**

ROZDZIAŁ III.
MINIMALIZACJA DOSTĘPU

1. Administrator stosuje ograniczenia dostępu do danych osobowych:
) prawne (zobowiązania do poufności, zakresy upoważnień);
) fizyczne (strefy dostępu, zamykanie pomieszczeń);
) logiczne (ograniczenia uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których rezydują dane osobowe),
2. Administrator dokonuje:
) okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż raz na rok;
) aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób oraz zmianach podmiotów przetwarzających.

ROZDZIAŁ IV.
MINIMALIZACJA CZASU

1. Administrator wdraża mechanizmy kontroli cyklu życia danych osobowych w Hotelu, w tym weryfikacji dalszej przydatności danych względem celów i terminów wskazanych w Rejestrze.
2. Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu, są usuwane z systemów informatycznych Administratora, jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów informatycznych przetwarzanych przez Administratora.

DZIAŁ VII.
BEZPIECZEŃSTWO

ROZDZIAŁ I.
POSTANOWIENIA OGÓLNE

1. Administrator zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez Hotel.
2. Administrator przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu:
) Administrator zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania – wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych.
) Administrator kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które prezentują.
) Administrator przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Administrator analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych, uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.
3. Administrator ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania.
4. Administrator ustala przydatność i stosuje takie środki i podejście, jak:
) szyfrowanie danych osobowych;
) inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
) środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

ROZDZIAŁ II.
ŚRODKI TECHNICZNE I ORGANIZACYJNE ZAPEWNIAJĄCE BEZPIECZEŃSTWO PRZETWARZANIA

1. Wdrożenie Polityki w Hotelu zapewnia:
) poufność – przetwarzane dane osobowe nie są udostępniane bądź ujawniane nieupoważnionym osobom lub podmiotom;
) integralność – powyższe dane nie zostają zmienione lub zniszczone w sposób nie autoryzowany;
    3) rozliczalność – możliwość jednoznacznego określenia pracowników lub podmiotów współpracujących uczestniczących w przetwarzaniu tych danych;
    4) dostępność – istnieje możliwość wykorzystania ich na żądanie, w założonym czasie, przez autoryzowany podmiot;
) autentyczność – zapewnienie, iż tożsamość podmiotu lub zasobu jest taka, jak deklarowana;
) niezaprzeczalność – uczestnictwo w całości lub części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie jest niepodważalne;
) niezawodność – zamierzone zachowania i skutki są spójne.
2. Realizację zamierzeń określonych w ust. 1 gwarantują przyjęte przez Hotel m.in. rozwiązania:

) wdrożenie procedur określających postępowanie osób zatrudnionych przy przetwarzaniu danych osobowych oraz ich odpowiedzialność za bezpieczeństwo tych danych;
) opracowanie procedur odtwarzania systemu w przypadku wystąpienia awarii;
) przeszkolenie użytkowników w zakresie bezpieczeństwa i ochrony danych osobowych;
) podejmowanie niezbędnych działań w celu likwidacji słabych ogniw w systemie zabezpieczeń;
) okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych;
) śledzenie osiągnięć w dziedzinie bezpieczeństwa systemów informatycznych oraz w miarę możliwości organizacyjnych i techniczno-finansowych - wdrażanie nowych narzędzi i metod pracy oraz sposobów zarządzania systemami informatycznymi, które będą służyły wzmocnieniu bezpieczeństwa danych osobowych.

3. Osoby przetwarzające dane osobowe w Hotelu muszą posiadać pisemne upoważnienie do przetwarzania danych wydane przez Administratora lub przez osobę przez niego upoważnioną, w przypadku danych osobowych przetwarzanych w sposób zautomatyzowany w porozumieniu z ASI.
4. Administrator prowadzi ewidencję upoważnień do przetwarzania danych osobowych.
5. Osoby przetwarzające dane osobowe w Hotelu podpisują również oświadczenie o zachowaniu poufności przetwarzanych danych, jeśli przy zawieraniu umowy o pracę lub umowy cywilnoprawnej z Hotelem nie składały tego rodzaju oświadczenia.
6. Administrator wprowadza Politykę Ochrony Danych Osobowych, z którym zapoznaje pracowników i współpracowników zobowiązując ich jednocześnie do jego przestrzegania.

DZIAŁ VIII.
PRZETWARZAJĄCY (PROCESOR)

1. Administrator może powierzyć przetwarzanie Danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej, zgodnie z wymogami wskazanymi dla takich umów w art. 28 RODO i tylko jeżeli są to dane, które może ujawnić bez naruszenia tajemnicy zawodowej.
2. Przed powierzeniem przetwarzania danych osobowych Administrator w miarę możliwości uzyskuje informacje o dotychczasowych praktykach podmiotu przetwarzającego dotyczących zabezpieczania danych osobowych.
3. Administrator rozlicza przetwarzających z wykorzystania innego podmiotu przetwarzającego, jak też z innych wymagań wynikających z zasad powierzenia danych osobowych.

TYTUŁ IV.
WSPÓŁADMINISTRATORZY
(ART. 26 RODO)

1. Jeżeli Administrator wspólnie ustala cele i sposoby przetwarzania z innym administratorem,

są oni współadministratorami.

2. W drodze wspólnych uzgodnień współadministratorzy w przejrzysty sposób określą odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw, oraz ich obowiązków w odniesieniu do podawania informacji, o których mowa w art. 13 i 14 RODO, chyba że przypadające im obowiązki i ich zakres określa prawo Unii lub prawo państwa członkowskiego, któremu administratorzy ci podlegają. W uzgodnieniach można wskazać punkt kontaktowy dla osób, których dane dotyczą.
3. Uzgodnienia, o których mowa w ust. 2, należycie odzwierciedlają odpowiednie zakresy obowiązków współadministratorów oraz relacje pomiędzy nimi a podmiotami, których dane dotyczą. Zasadnicza treść uzgodnień jest udostępniana podmiotom, których dane dotyczą.
4. Niezależnie od uzgodnień, o których mowa w ust. 2, osoba, której dane dotyczą, może wykonywać przysługujące jej prawa wynikające z niniejszego rozporządzenia wobec każdego z administratorów.
5. Administrator dochowuje wszelkich starań w celu określenia czy nie zachodzi współadministrowanie przetwarzaniem danych osobowych.

1. nagrania obrazu zawierające dane osobowe podlegają zniszczeniu, o ile przepisy odrębne nie stanowią inaczej.
2. Administrator informuje pracowników, inne osoby o stosowaniu monitoringu wizyjnego, w sposób przyjęty u Administratora.
3. Administrator przed dopuszczeniem nowo zatrudnionego pracownika do pracy lub wykonywania innych czynności na rzecz Administratora przekazuje mu na piśmie informacje, o celach, zakresie oraz sposobie zastosowania monitoringu.