# POLITYKA
# OCHRONY DANYCH
# OSOBOWYCH

– Centrum Twojego Zdrowia (Guzik MED) –

Kraków 2019

# Spis treści

# Wykaz skrótów i definicji

| | |
|---|---|
| **Rozporządzenie, RODO** | 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 95/36/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119) z późn. zm. |
| **Ustawa** | Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000) |
| **Organ nadzorczy** | Prezes Urzędu Ochrony Danych Osobowych |
| **Administrator** | osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych |
| **Organizacja** | Specjalistyczny Gabinet Lekarski Bartłomiej Guzik MED – z zakładem leczniczym Centrum Twojego Zdrowia z siedzibą w Krakowie (31-526) przy ul. Kieleckiej 2, NIP: 6762080733 |
| **dane osobowe** | informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Mogą obejmować w szczególności (lecz nie wyłącznie) 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 |
| **dane szczególnych kategorii** | 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 (art. 9 ust. 1 RODO) |
| **przetwarzanie** | operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka 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 |
| **Polityka Ochrony Danych Osobowych, Polityka** | dokument określający generalne zasady przetwarzania danych osobowych w Organizacji |
| **Procedura** | dokument wdrożony do stosowania w Organizacji zawierający wskazany tryb postępowania w poszczególnych obszarach działań Organizacji w zakresie danych osobowych |
| **Rejestr, RCPD** | Rejestr Czynności Przetwarzania Danych Osobowych (art. 30 RODO) |
| **Osoba odpowiedzialna** | osoba wyznaczona w ramach struktury Organizacji, posiadająca odpowiednią wiedzę, kompetencję i uprawnienia konieczne do wykonywania działań określonych Polityką lub Procedurą |
| **Inspektor Ochrony Danych, IOD** | podmiot wyznaczony w Organizacji i spełniający kryteria wskazane w art. 37 RODO oraz posiadający status i wykonujący zadania określone w art. 38-39 RODO |
| **Podmiot przetwarzający, Procesor** | zewnętrzny dostawca towarów lub usług lub klient lub kontrahent Organizacji, który przetwarza dane osobowe w imieniu Organizacji |
| **Kontrahent** | osoba fizyczna lub prawna, która jest dostawcą usług lub towarów dla Organizacji |

| | |
|---|---|
| **Pracownik** | osoba fizyczna osoba zatrudniona na podstawie umowy o pracę w rozumieniu art. 2 ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy |
| **Współpracownik** | osoba fizyczna współpracująca z Organizacją na podstawie umowy cywilnoprawnej w rozumieniu ustawy z dnia 23 kwietnia 1964 r. - Kodeks cywilny |
| **Personel** | ogół Pracowników i Współpracowników w Organizacji |
| **Uprawnienia** | prawa osób, których dane dotyczą, przyznane na mocy Rozporządzenia obejmujące w szczególności: prawo do informacji, prawo dostępu do danych, prawo do sprostowania i/lub uzupełnienia danych, prawo do usunięcia danych, prawo do ograniczenia przetwarzania danych, prawo do przenoszenia danych oraz prawo do sprzeciwu |
| **EOG** | Europejski Obszar Gospodarczy zdefiniowany w Porozumieniu o Europejskim Obszarze Gospodarczym (Dz. U.UE L z dnia 3 stycznia 1994 r. z późn. zm.) Unia Europejska oraz Norwegia, Islandia, Lichtenstein |
| **Państwo trzecie** | Państwo poza Europejskim Obszarem Gospodarczym |
| **Organizacja międzynarodowa** | Organizacja 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 |
| **system informatyczny** | zespół współpracujących ze sobą urządzeń, programów, aplikacji, systemów i procedur przetwarzania informacji oraz narzędzi programowych zastosowanych w celu przetwarzania danych |
| **Użytkownik systemu informatycznego** | osoba upoważniona do przetwarzania danych osobowych w systemie informatycznym Organizacji. Użytkownikiem systemu informatycznego może być Pracownik lub Współpracownik |

| | |
|---|---|
| **Wewnętrzna sieć informatyczna** | Lokalna sieć komputerowa wraz z serwerem plików |
| **Instrukcja** | Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, wdrożona w Organizacji |

# 1. Wstęp

Organizacja powołuje niniejszą Politykę jako podstawowy dokument dotyczący ochrony danych osobowych w Organizacji, który określa funkcjonowanie całego systemu powiązanych ze sobą zasad, założeń, Procedur i innych dokumentów dotyczących ochrony danych osobowych.

Celem Polityki jest określenie oraz wdrożenie zasad bezpieczeństwa i ochrony danych osobowych przetwarzanych w Organizacji oraz Procedur postępowania z danymi osobowymi w procesie ich przetwarzania, co powoduje, że Organizacja odpowiednio chroni dane osobowe, a realizując tą ochronę pozostaje w zgodzie z przepisami prawa i zabezpiecza prawa podmiotów, których dane przetwarza.

Polityka określa zakres zadań i odpowiedzialności osób przetwarzających dane osobowe w Organizacji. Ponadto reguluje zasady i formy powierzenia przetwarzania danych osobowych, w tym zasady upoważniania personelu do przetwarzania danych, przekazania danych podmiotowi przetwarzającemu oraz udostępniania danych do innego administratora.

Polityka obejmuje również regulacje dotyczące zasad sporządzania i prowadzenia rejestru czynności przetwarzania danych oraz kwestię zarządzania ryzykiem w procesach przetwarzania danych osobowych. W Polityce określono także ogólne zasady: ustalania okresów przetwarzania danych osobowych, realizacji uprawnień osób, których dane dotyczą, zgłaszania naruszeń ochrony danych osobowych, przekazywania danych do Państw trzecich lub Organizacji międzynarodowych, dla których sporządzono szczegółowe Procedury postępowania.

Polityka będzie monitorowana pod kątem jej efektywności oraz uzupełniana i modyfikowana na gruncie zgodności z Rozporządzeniem i Ustawą, praktyki działalności Organu nadzorczego, wykształconej po wejściu w życie Rozporządzenia oraz Ustawy (a w przyszłości także innych aktów prawnych związanych z ochroną danych osobowych). Polityka uwzględnia również postanowienia zawarte w Kodeksie Postępowania dla Sektora Ochrony Zdrowia wydanego zgodnie z art. 40 RODO dotyczącego Podmiotów Wykonujących Działalność Leczniczą i Podmiotów Przetwarzających, co stanowi okoliczność potwierdzającą wywiązywanie się z obowiązków nałożonych przez RODO na Administratora, który działa na rynku podmiotów wykonujących działalność leczniczą i służy tym samym realizacji zasady rozliczalności.

# 2. Zakres zadań i odpowiedzialności

## 2.1. Wspólnicy Organizacji

2.1.1. Wspólnicy Organizacji są odpowiedzialni za wdrożenie i utrzymanie Polityki oraz za nadzór i monitorowanie jej przestrzegania, w tym zakresie Wspólnicy Organizacji w szczególności:

a. wyznaczają spośród siebie Osobę odpowiedzialną,

b. w razie potrzeby, zapewnią do konsultacji osobę lub osoby z zewnątrz Organizacji dysponujących odpowiednią wiedzą i doświadczeniem w zakresie ochrony danych osobowych,

c. zatwierdzają strategię i podejmują decyzje dotyczące ochrony danych osobowych w Organizacji,

d. nadzorują przygotowanie dokumentacji związanej z ochroną danych osobowych w Organizacji,

e. akceptują dokumenty dotyczące ochrony danych osobowych w Organizacji, w tym Procedury wraz z załącznikami, Rejestr i wyniki szacowania ryzyka w formie uchwały,

f. podejmują decyzje w innych sprawach z zakresu ochrony danych osobowych pojawiających się w Organizacji podczas jej działalności.

## 2.2. Inspektor Ochrony Danych

2.2.1. Wspólnicy Organizacji dokonali analizy przepisów RODO pod kątem obowiązku powołania Inspektora Ochrony Danych w Organizacji i stwierdził, iż Organizacja nie jest zobowiązana do wyznaczenia IOD, gdyż nie spełnia przesłanek, o których mowa w Rozporządzeniu, zgodnie z którymi Administrator jest obowiązany wyznaczyć IOD, wskazanych poniżej:

a. przetwarzania dokonuje organ lub podmiot publiczny (z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości),

b. główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę,

c. główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych albo danych osobowych dotyczących wyroków skazujących i naruszeń prawa.

## 2.3. Osoba odpowiedzialna

2.3.1. Wspólnicy Organizacji wyznaczają spośród siebie osobę, która będzie odpowiedzialna za ochronę danych osobowych w Organizacji oraz będzie ona realizowała zadania określone w poszczególnych Procedurach. Osoba odpowiedzialna nie może być jednak utożsamiana z IOD.

## 2.4. Personel

2.4.1. Za stosowanie i przestrzeganie zasad określonych w niniejszej Polityce odpowiedzialni są wszyscy członkowie Personelu Organizacji. Osoby te zobowiązane są do zgłaszania za pośrednictwem przełożonych lub bezpośrednio do Osoby odpowiedzialnej wszystkich przypadków wykrycia incydentów naruszenia ochrony danych osobowych, uzyskania żądania lub informacji od osób, których dane dotyczą oraz konieczności powierzenia przetwarzania danych osobowych, a także wszystkich innych sytuacji w których powezmą wątpliwość związaną z przetwarzaniem lub ochroną danych osobowych.

# 3. Zasady przetwarzania danych osobowych w Organizacji

## 3.1. Zasady ogólne

3.1.1. Organizacja w procesach przetwarzania danych osobowych przestrzega następujących zasad:

a. legalizmu tj. przetwarza dane osobowe w oparciu o podstawę prawną i zgodnie z prawem, a także dba o ochronę prywatności,

b. rzetelności i transparentności tj. przetwarza dane osobowe rzetelnie i uczciwie, w sposób przejrzysty dla osób, których dane dotyczą, umożliwiając tym osobom, wykonywanie ich praw i prawa te realizuje,

c. minimalizmu, w tym adekwatności i czasowości tj. przetwarza dane osobowe w konkretnych celach oraz jedynie te dane, które są niezbędne dla realizacji celu przetwarzania oraz przez odpowiedni do tego okres,

d. prawidłowości tj. kontroluje czy przetwarza jedynie prawidłowe dane osobowe osoby, której dane dotyczą,

e. bezpieczeństwa, w tym integralności i poufności danych tj. przetwarza dane osobowe zapewniając odpowiedni poziom bezpieczeństwa tych danych i w tym zakresie podejmuje stałe działania zmierzające do poprawy zabezpieczeń danych,

f. rozliczalności tj. dokumentuje to, w jaki sposób spełnia obowiązki nałożone wymogami RODO, aby w każdej chwili móc wykazać zgodność postępowania z tymi wymogami, a nadto żeby potwierdzić, iż przyjęte metody działania są skuteczne.

## 3.2. Podstawy przetwarzania

3.2.1. Organizacja przetwarza dane osobowe tylko wówczas gdy posiada wynikającą z RODO podstawę prawną do ich przetwarzania.

3.2.2. Osoba odpowiedzialna ustala ogólne podstawy prawne przetwarzania danych osobowych w precyzyjny i czytelny sposób dla poszczególnych procesów przetwarzania danych osobowych.

3.2.3. Podstawa prawna przetwarzania danych osobowych w Organizacji, jest określana w szczególności zgodnie z wytycznymi określonymi poniżej:

a. w przypadku, gdy podstawą prawną jest zgoda osoby, której dane dotyczą – określa się jej zakres, podając w jej treści co najmniej dane Administratora i cel przetwarzania,

b. w przypadku, gdy podstawą prawną jest prawo – podaje się konkretny przepis prawa i inne dokumenty, np. umowę, porozumienie,

c. w przypadku, gdy podstawą są żywotne interesy Organizacji – określa się kategorie zdarzeń, w których te interesy się materializują,

d. w przypadku, gdy podstawą jest uzasadniony cel Organizacji – podaje się konkretny cel, np. marketing własny, dochodzenie roszczeń.

3.2.4. Szczegółowe zasady określania postawy prawnej przetwarzania danych osobowych uregulowane zostały w odrębnej Procedurze wskazanej w pkt. 7 Polityki.

## 3.3. Bezpieczeństwo

3.3.1. Organizacja zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób, których dane dotyczą podczas przetwarzania ich danych osobowych w procesach, które występują w Organizacji.

3.3.2. Organizacja w tym celu przeprowadza i dokumentuje szacowanie ryzyka oraz dokonuje analizy adekwatności środków bezpieczeństwa danych osobowych. W szczególności, Organizacja:

a. przeprowadza szacowanie ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych,

b. ustala możliwe do zastosowania środki bezpieczeństwa (prawne, organizacyjne fizyczne i informatyczne) i ocenia koszt ich wdrażania. Organizacja ustala przydatność, a następnie podejmuje decyzję o stosowaniu środków, w szczególności środków takich jak: pseudonimizacja lub szyfrowanie danych osobowych, a także inne środki cyberbezpieczeństwa, składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania oraz zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,

c. zapewnia regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania w systemach informatycznych,

d. dostarcza osobom przetwarzającym dane osobowe w Organizacji odpowiedni stan wiedzy o bezpieczeństwie ochrony danych osobowych, cyberbezpieczeństwie i ciągłości działania poprzez przeprowadzanie szkoleń (również ze wsparciem podmiotów wyspecjalizowanych w prawie ochrony danych osobowych i bezpieczeństwie w systemach informatycznych).

3.3.3. Organizacja odrębnie określa zakres stosowanych przez nią środków bezpieczeństwa danych osobowych. W tym celu Organizacja wdraża odrębny dokument zawierający opisy stosowanych przez nią środków zabezpieczenia danych osobowych, który stanowi Załącznik nr I do Polityki.

3.3.4. Niezależenie od regulacji, o której mowa w pkt. 3.3.3, Organizacja reguluje zasady funkcjonowania i korzystania z systemu informatycznego. W tym celu Organizacja wdraża Instrukcję zarządzania systemem informatycznym, która stanowi Załącznik nr II do Polityki.

## 3.4. Ochrona prywatności

3.4.1. Organizacja przestrzega zasad *privacy by design* (czyli projektowanie prywatności) oraz *privacy by default* (czyli domyślną ochronę danych).

3.4.2. Organizacja realizując powyżej wskazane zasady (zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania) wdraża odpowiednie środki techniczne i organizacyjne, które mają na celu skuteczną realizację zasad ochrony danych osobowych, takich jak minimalizacja tych danych, a także zapewnienie niezbędnych zabezpieczeń w procesach przetwarzania danych osobowych, tak by spełnić wymogi RODO oraz chronić prawa osób, których dane dotyczą.

3.4.3. W tym zakresie Organizacja uwzględnia stan wiedzy technicznej, koszt wdrażania odpowiednich środków oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko

naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania danych osobowych.

3.4.4. Organizacja podejmuje odpowiednie środki zabezpieczeń danych osobowych, które szczegółowo wskazuje w RCPD, aby przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania (odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności). Stosowane przez Organizację środki zabezpieczeń zapewniają również, że domyślnie dane osobowe nie są udostępniane osobom do tego nieuprawnionym.

# 4. Forma powierzenia przetwarzania danych osobowych

## 4.1. Upoważnienie osób w Organizacji do przetwarzania danych

4.1.1. Osoby, które mogą przetwarzać w imieniu Organizacji przetwarzane przez nią dane osobowe to Pracownicy, w szczególnych przypadkach również Współpracownicy.

4.1.2. Organizacja wskazuje konkretne osoby, które w ramach jej struktury mogą w jej imieniu przetwarzać dane osobowe.

4.1.3. Każda osoba przetwarzająca dane osobowe w Organizacji, przed dopuszczeniem do przetwarzania tych danych, uzyskuje od Osoby odpowiedzialnej pisemne upoważnienie do przetwarzania danych, zawierające zakres danych udostępnionych do przetwarzania oraz okres przetwarzania, którego wzór stanowi Załącznik nr III do Polityki.

4.1.4. Organizacja okresowo, nie rzadziej niż raz w roku, weryfikuje zakres i okres, przez który osoba przetwarzająca dane osobowe może te dane przetwarzać.

4.1.5. Osoby przetwarzające dane osobowe odpowiedzialne są za:

a. przetwarzanie danych osobowych w zakresie upoważnienia otrzymanego od Organizacji,

b. przetwarzanie danych osobowych zgodnie z Polityką i Procedurami,

c. przestrzeganie zasad przetwarzania Danych osobowych przyjętych w Organizacji,

d. niezwłocznego informowania Wspólników lub Osoby odpowiedzialnej o wszelkich nieprawidłowościach dotyczących bezpieczeństwa przetwarzania danych osobowych w Organizacji.

4.1.6. Osoba odpowiedzialna prowadzi wykaz osób upoważnionych do przetwarzania danych osobowych w Organizacji, którego wzór stanowi Załącznik nr IV do Polityki, oraz odpowiada za archiwizację wydanych upoważnień.

## 4.2. Powierzenie danych podmiotowi przetwarzającemu

4.2.1. Każdy członek Personelu, przed przekazaniem informacji do Kontrahenta, powinien sprawdzić czy w ramach przekazywania informacji może nastąpić również powierzenie przetwarzania danych osobowych tj. czy podmiot, któremu przekazywane są dane osobowe otrzyma również wytyczne o celu i sposobie postępowania z danymi osobowymi osób, których Administratorem jest Organizacja (co oznacza, że Podmiot przetwarzający sam nie będzie decydował ani o celu ani o sposobie przetwarzania przekazanych danych osobowych).

4.2.2. W przypadku wątpliwości w zakresie potwierdzenia warunków, o których mowa w pkt. 4.2.1. członek Personelu powinien przed przekazaniem danych skontaktować się z Osobą odpowiedzialną.

4.2.3. W przypadku potwierdzenia, że w ramach przekazywania informacji dojdzie do powierzenia danych osobowych, wówczas członek Personelu lub Osoba odpowiedzialna zobowiązani są do ustalenia czy przekazywanie przetwarzania danych osobowych będzie miało miejsce w ramach obszaru EOG czy poza nim.

4.2.4. Jeżeli przekazywanie danych osobowych dotyczy obszaru EOG, osoba przetwarzająca dane osobowe w Organizacji przedstawia Procesorowi umowę, ewentualnie klauzulę powierzenia przetwarzania określającą przedmiot i czas trwania przetwarzania, charakter i cele przetwarzania, rodzaj danych osobowych i kategorie osób, których dane dotyczą, oraz uwzględnia konkretne zadania i obowiązki Podmiotu przetwarzającego w kontekście planowanego przetwarzania. Wzór umowy stanowi Załącznik nr V do Polityki, wzór klauzuli powierzenia przetwarzania wprowadzanej do umowy stanowi Załącznik nr VI do Polityki. W przypadku powzięcia wątpliwości, który ze środków prawnych, wskazanych w zdaniu poprzednim, należy zastosować w danej sytuacji, osoba powierzająca dane osobowe powinna skontaktować się z Osobą odpowiedzialną.

4.2.5. Jeżeli przekazywanie danych osobowych ma nastąpić poza obszar EOG to osoba przetwarzająca dane osobowe w Organizacji postępuje zgodnie z zasadami określonymi w Procedurze przekazywania danych do Państw trzecich lub Organizacji międzynarodowych wskazanej w pkt. 10 Polityki.

4.2.6. Organizacja powierzając czynności przetwarzania danych osobowych, współpracuje wyłącznie z Podmiotami przetwarzającymi, które zapewniają wystarczające gwarancje (w szczególności jeżeli chodzi o wiedzę fachową, wiarygodność i zasoby) wdrożenia środków technicznych i organizacyjnych odpowiadających wymogom RODO.

4.2.7. Osoba odpowiedzialna prowadzi wykaz podmiotów, którym powierzono przetwarzanie danych osobowych . Wzór wykazu stanowi Załącznik nr VII do Polityki.

## 4.3. Udostępnianie danych do innego administratora

4.3.1. Każda osoba przetwarzająca dane osobowe w Organizacji, przekazująca informacje do Kontrahenta, powinna sprawdzić czy w ramach przekazywania informacji udostępnia Kontrahentowi dane osobowe tj. czy podmiot, któremu udostępniane są dane osobowe sam będzie decydował o celu i sposobie postępowania z danymi osobowymi osób, których Administratorem jest Organizacja (co oznacza, że Kontrahent sam będzie decydował zarówno o celu, jak i o sposobie przetwarzania udostępnionych danych osobowych).

4.3.2. W przypadku wątpliwości w zakresie potwierdzenia warunków, o których mowa w pkt. 4.3.1. osoba przetwarzająca dane powinna przed przekazaniem danych skontaktować się z Osobą odpowiedzialną.

4.3.3. W przypadku ustalenia, że w ramach przekazywania informacji do Kontrahenta, Kontrahent jest również Administratorem przekazanych mu danych osobowych wówczas członek Personelu w Organizacji przedstawia Kontrahentowi klauzulę udostępnienia danych osobowych, której wzór stanowi Załącznik nr VIII do Polityki.

# 5. Rejestr czynności przetwarzania danych

5.1. Rejestr pełni rolę mapy przetwarzania danych osobowych w Organizacji i jest jednym z podstawowych elementów umożliwiających realizację zasady rozliczalności określonej przez RODO, spełnia on również funkcję informacyjną, gdyż stanowi źródło informacji o procesach przetwarzania danych w Organizacji.

5.2. Organizacja prowadzi Rejestr, w którym inwentaryzuje i monitoruje czynności przetwarzania danych osobowych.

5.3. W Rejestrze dla każdej czynności przetwarzania danych, którą Organizacja uznała za odrębną, Organizacja wskazuje co najmniej: nazwę czynności przetwarzania, cel przetwarzania, podstawę przetwarzania, osoby, które biorą udział w procesie, kategorie osób, kategorie danych osobowych, szczególne kategorie danych, kategorie odbiorców danych osobowych, sposób pozyskiwania danych, sposób przetwarzania danych, okres przechowywania danych, powierzenie danych osobowych, transfer do Państwa trzeciego lub Organizacji międzynarodowej, ogólny opis środków bezpieczeństwa ochrony danych osobowych (z rozróżnieniem na środki prawne, organizacyjne, fizyczne oraz informatyczne).

5.4. Rejestr prowadzony jest przez Osobę odpowiedzialną, która weryfikuje nie rzadziej niż raz na rok treść Rejestru, uzupełnia go i aktualizuje. W tym celu współdziała z drugim Wspólnikiem Organizacji i członkami Personelu.

5.5. Rejestr prowadzony jest w formie tabeli w pliku exel lub w formie papierowej, z oznaczeniem wersji i stanem na miesiąc i rok sporządzania Rejestru.

5.6. Wzór Rejestru stanowi Załącznik nr IX do Polityki.

# 6. Zarządzanie ryzykiem

6.1. Dla zapewnienia skutecznej ochrony praw i interesów osób, których dane są przetwarzane, RODO wprowadza podejście oparte na ryzyku, co oznacza, że Organizacja sama określa cele i środki stosowane w procesach przetwarzania danych osobowych w Organizacji.

6.2. W celu spójnego i przejrzystego zarządzania ryzykiem, podzielono proces szacowania ryzyka na cztery etapy tj.:

a. ustalenie kontekstu przetwarzania danych osobowych,

b. identyfikację wymagań dotyczących procesów przetwarzania danych w kontekście celów oraz zastosowanych środków bezpieczeństwa,

c. szacowanie ryzyka na podstawie zidentyfikowanych zagrożeń, prawdopodobieństwa zdarzeń oraz skutków ewentualnego naruszenia,

d. określenie zasad postępowania z ryzykiem, w tym prowadzenia ogólnej oceny ryzyka oraz oceny skutków dla ochrony danych.

6.3. Organizacja przeprowadza i dokumentuje efekty szacowania ryzyka.

6.4. Organizacja dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z wynikiem szacowania ryzyka, ryzyko naruszenia praw i wolności osób jest wysokie.

6.5. Szczegółowy tryb postępowania z ryzykiem został określony w Procedurze zarządzania ryzykiem w procesach przetwarzania danych osobowych, która stanowi Załącznik nr X do Polityki.

# 7. Zasady ustalania podstawy prawnej, okresów przetwarzania, weryfikowania, usuwania danych osobowych

7.1. Organizacja ustala reguły postępowania w zakresie ustalania podstawy prawnej, wyznaczania okresów przetwarzania danych osobowych oraz w przedmiocie następczego weryfikowania i usuwania lub anonimizowania danych osobowych co powoduje, że w Organizacji wdrożone jest spójne i skuteczne podejście do zarządzania danymi osobowymi w tym zakresie.

7.2. W tym celu Organizacja wprowadza do stosowania Procedurę, która zawiera:

a. opis rozwiązań, które Organizacja wprowadza w celu umożliwienia odpowiedniej realizacji obowiązków wynikających z Rozporządzenia,

b. opis działań szczegółowych w stosunku do określania podstawy prawnej przetwarzania danych osobowych,

c. opis działań szczegółowych w zakresie określania okresu przechowania danych osobowych,

d. zasady zmiany podstawy prawnej przetwarzania danych osobowych,

e. opis działań szczegółowych w stosunku do weryfikowanych i usuwanych danych osobowych.

7.3. Szczegółowy tryb postępowania w sprawie ustalania okresów przetwarzania danych osobowych został określony w Procedurze ustalania podstawy prawnej, okresów przetwarzania, weryfikowania i usuwania danych osobowych, która stanowi Załącznik nr XI do Polityki.

# 8. Zasady realizacji uprawnień osób, których dane dotyczą

8.1. Organizacja ustala reguły postępowania w zakresie realizacji Uprawnień osób, których dane dotyczą, mających swoje źródło w regulacjach prawa ochrony danych osobowych co powoduje, że w Organizacji wdrożone jest spójne i skuteczne podejście do realizacji Uprawnień w stosunku do danych osobowych.

8.2. W celu realizacji Uprawnień Organizacja wprowadza do stosowania Procedurę, która zawiera:

a. opis wytycznych dotyczących spełniania przez Organizację obowiązku informacyjnego wobec osób których dane dotyczą,

b. opis rozwiązań w zakresie obsługi Uprawnień, których Organizacja przestrzega w każdym przypadku realizacji Uprawnień.

8.3. Szczegółowy tryb postępowania w sprawie realizacji Uprawnień osób, których dane dotyczą został określony w Procedurze w zakresie realizacji uprawnień osób, których dane dotyczą, stanowiącej Załącznik nr XII do Polityki.

# 9. Zasady zgłaszania naruszeń ochrony danych osobowych

9.1. Organizacja ustala reguły postępowania w zakresie wykrywania oraz reagowania na naruszenia ochrony danych osobowych co powoduje, że w Organizacji wdrożone jest spójne i skuteczne podejście do zarządzania przypadkami naruszenia danych zarówno pod względem zapobiegania i przeciwdziałania naruszeniom, jak i pod względem podejmowania odpowiedniej i szybkiej reakcji na przypadki ich występowania.

9.2. W tym celu Organizacja wprowadza do stosowania Procedurę, która zawiera:

a. opis rozwiązań, które Organizacja wprowadza w celu umożliwienia odpowiedniej realizacji obowiązków wynikających z Rozporządzenia,

b. opis działań koniecznych do przeprowadzenia w związku z podejrzeniami wystąpienia naruszeń ochrony danych osobowych.

9.3. Szczegółowy tryb postępowania w sprawie zgłaszania naruszeń ochrony danych osobowych został określony w Procedurze reagowania na naruszenia ochrony danych osobowych, która stanowi Załącznik nr XIII do Polityki.

# 10. Zasady przekazywania danych do Państw trzecich lub Organizacji międzynarodowych

10.1. Organizacja ustala reguły postępowania w zakresie przekazywania danych osobowych do Państw trzecich lub Organizacji międzynarodowych co powoduje, że w Organizacji wdrożone jest spójne i skuteczne podejście do przekazywania danych osobowych do Państw trzecich lub Organizacji międzynarodowych.

10.2. W tym celu Organizacja wprowadza do stosowania Procedurę, która zawiera:

a. opis ogólnych zasad przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych,

b. opis rozwiązań, które Organizacja wprowadza w celu umożliwienia odpowiedniej realizacji obowiązków wynikających z Rozporządzenia (m.in. weryfikacja podstawy prawnej na jakiej przekazywane są dane osobowe do Państw trzecich lub Organizacji międzynarodowych),

c. opis działań szczegółowych koniecznych do przeprowadzenia w celu podjęcia odpowiedniej decyzji w stosunku do przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych.

10.3. Szczegółowy tryb postępowania w sytuacji przekazywania danych do Państw trzecich lub Organizacji międzynarodowych został określony w Procedurze przekazywania danych do Państw trzecich lub Organizacji międzynarodowych, która stanowi Załącznik nr XIV do Polityki.

# 11. Szkolenia

11.1. Organizacja prowadzi działania mające na celu pogłębienie świadomości członków Personelu w zakresie przetwarzania danych osobowych, w tym w szczególności Organizacja prowadzi obowiązkowe szkolenia dla wszystkich członków Personelu z zakresu przetwarzania danych osobowych.

11.2. Organizacja przewiduje, że każdy z członków Personelu zostanie przeszkolony przed dopuszczeniem go do pełnienia obowiązków oraz będzie szkolony cykliczne, co najmniej raz w roku.

11.3. W ramach realizacji powyższych założeń, Organizacja może organizować szkolenia wewnętrzne prowadzone przez osobę posiadającą odpowiednie doświadczenie z zakresu ochrony danych osobowych lub z pomocą wyspecjalizowanego podmiotu zewnętrznego w tym zakresie. Dodatkowo Organizacja może korzystać z oferty szkoleń zewnętrznych, w tym w szczególności organizowanych przez Organ nadzorczy.

11.4. Członkowie Personelu potwierdzają swój udział w szkoleniu z zakresu danych osobowych poprzez złożenie oświadczenia, którego wzór stanowi Załącznik nr XV do Polityki.

# 12. Postanowienia końcowe

12.1. Niniejsza Polityka obowiązuje w Organizacji od 1 czerwca 2019 roku. Dane wprowadzone do treści Polityki lub do Załączników potwierdzają stan faktyczny na dzień uchwały Wspólników Organizacji wprowadzającej je w życie.

12.2. Personel zostanie powiadomiony o treści Polityki i Załączników. Wspólnicy Organizacji zobowiążą Personel do przestrzegania obowiązków wynikających z niniejszej Polityki oraz do zachowania poufności danych osobowych przetwarzanych w Organizacji na podstawie oświadczenia, które stanowi Załącznik nr XVI do Polityki. Ponad to każdy nowy członek Personelu zostanie zapoznany z treścią Polityki i Załączników przed dopuszczeniem go do pełnienia obowiązków w Organizacji.

12.3. Wszystkie Załączniki do niniejszej Polityki stanowią jej integralną część.

12.4. Zważywszy, iż RODO wprowadza nowe instytucje prawa oraz iż do dnia rozpoczęcia obowiązywania Polityki nie zdążyły się ukształtować jednolite poglądy doktryny ani judykatury, Organizacja będzie monitorować kształtującą się w tym zakresie praktykę, a gdy okaże się konieczne wprowadzenie zmian do Polityki lub Załączników, podejmie stosowne działania w tym zakresie.

# 13. Wykaz załączników

13.1. Niniejsza Polityka zawiera następujące załączniki:

a. Załącznik nr I – Środki zabezpieczenia danych osobowych
b. Załącznik nr II – Instrukcja zarządzania systemem informatycznym
c. Załącznik nr III – Wzór upoważnienia do przetwarzania danych osobowych
d. Załącznik nr IV – Wzór wykazu osób upoważnionych do przetwarzania danych w Organizacji
e. Załącznik nr V – Wzór umowy powierzenia przetwarzania danych osobowych
f. Załącznik nr VI – Wzór klauzuli powierzenia przetwarzania danych osobowych
g. Załącznik nr VII – Wzór wykazu podmiotów, którym powierzono przetwarzanie danych osobowych
h. Załącznik nr VIII – Wzór klauzuli udostępnienia danych osobowych innemu administratorowi danych osobowych
i. Załącznik nr IX – Wzór rejestru czynności przetwarzania danych osobowych
j. Załącznik nr X – Procedura zarządzania ryzykiem w procesach przetwarzania danych osobowych
k. Załącznik nr XI – Procedura ustalania podstawy prawnej, okresów przetwarzania, weryfikowania i usuwania danych osobowych
l. Załącznik nr XII – Procedura w zakresie realizacji uprawnień osób, których dane dotyczą
m. Załącznik nr XIII – Procedura reagowania na naruszenia ochrony danych osobowych
n. Załącznik nr XIV – Procedura przekazywania danych do Państw trzecich lub Organizacji międzynarodowych
o. Załącznik nr XV – Wzór oświadczenia o odbyciu szkolenia z zakresu danych osobowych
p. Załącznik nr XVI – Wzór oświadczenia dotyczącego przestrzegania obowiązków wynikających z niniejszej Polityki oraz zachowania poufności danych osobowych przetwarzanych w Organizacji