09.04.2024 r.

POLITYKA OCHRONY

DANYCH OSOBOWYCH

KONWENT OJCÓW BONIFRATRÓW

Bonifraterska 11, 32-031 Mogilany, Konary

SPIS TREŚCI

1. Wstęp

1.1. KONWENT OJCÓW BONIFRATRÓW (dalej „**Administrator**") wdrożył niniejszą Politykę ochrony danych osobowych (dalej „**Polityka**") w celu zapewnienia prawidłowego przetwarzania danych osobowych uwzgledniającego obowiązki nałożone przepisami 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 (dalej „**RODO**") oraz polskimi regulacjami prawnymi w zakresie ochrony danych osobowych.

1.2. Polityka określa zasady przetwarzania danych osobowych, warunki techniczne i organizacyjne zapewniające ich ochronę oraz obowiązki, jakie Administrator zobowiązuje się wypełniać, aby zapewnić zgodność prowadzonej działalności z obowiązującymi przepisami o ochronie danych osobowych.

1.3. Obowiązki określone w Polityce mają zastosowanie do wszystkich danych osobowych przetwarzanych przez Administratora, zarówno w formie papierowej jak i elektronicznej.

1.4. Polityka obowiązuje wszystkich pracowników i współpracowników stanowiących personel Administratora (dalej „**Personel**").

1.5. Personel Administratora jest zobowiązany do przestrzegania zasad wynikających z Polityki oraz dokumentów związanych z Polityką.

1.6. Nieprzestrzeganie obowiązków wynikających z Polityki oraz dokumentów związanych z Polityką może skutkować odpowiedzialnością dyscyplinarną lub cywilnoprawną pracownika zgodnie z kodeksem pracy, a w przypadku umów cywilnoprawnych – odpowiedzialnością cywilnoprawną.

1.7. Polityka zatwierdzana jest przez Administratora i podawana do wiadomości Personelu jako dokument do użytku wewnętrznego Administratora.

1.8. Polityka podlega przeglądowi raz w roku lub w razie zmian przepisów prawa. W przypadku konieczności Polityka podlega aktualizacji.

2. Podstawowe definicje

2.1. **Administrator** - KONWENT OJCÓW BONIFRATRÓW, Bonifraterska 11, 32-031 Mogilany, Konary;

2.2. **Atrybuty bezpieczeństwa:**

- Poufność – zapewnienie, że dane osobowe są udostępniane jedynie osobom upoważnionym,
- Integralność – zapewnienie zupełnej dokładności i kompletności danych osobowych oraz metod ich przetwarzania,
- Dostępność – zapewnienie, że osoby upoważnione mają dostęp do danych osobowych tylko wtedy, gdy istnieje taka potrzeba.

2.3. **Dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować,

w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

2.4. **Naruszenie ochrony danych osobowych** – 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;

2.5. **Personel** – osoby zatrudnione na podstawie stosunku pracy, umów cywilnoprawnych (umowa o dzieło, umowa zlecenia), przedsiębiorcy wykonujący działalność osobiście i jednoosobowo, osoby odbywające praktyki, stażyści, osoby skierowane do pracy w ramach umów z agencjami pracy tymczasowej wykonujące prace związane z przetwarzaniem danych osobowych u Administratora.

2.6. **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;

2.7. **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;

2.8. **Szczególne kategorie danych osobowych** – oznaczają dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby oraz dane genetyczne i dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej;

2.9. Współadministrator – oznacza podmiot, który wspólnie z Administratorem ustala cele i sposoby przetwarzania danych osobowych

2.10. Wykaz skrótów:

- **UODO** – Urząd Ochrony Danych Osobowych - organ powołany do spraw ochrony danych osobowych,
- **RODO** – ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie

swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

- **Polityka** – niniejsza Polityka Ochrony Danych Osobowych.

3. Zasady postępowania z dokumentami

3.1. W celu realizacji postanowień Polityki wdrożone zostaną odpowiednie procedury, instrukcje, rejestry, zasady lub szczegółowe polityki regulujące wykonanie poszczególnych obowiązków prawnych.

3.2. Podczas wdrażania ww. dokumentów należy w szczególności określić:

- Sposób przyjęcia dokumentu przez Administratora,
- Odbiorców dokumentu oraz sposób informowania ich o dokumencie,
- Obowiązek przeglądu i ewentualnej aktualizacji dokumentu,
- Sposób weryfikacji stosowania obowiązków wynikających z dokumentu.

3.3. W stosownych wypadkach Administrator opracowuje wewnętrzne materiały informacyjne i edukacyjne dla Personelu lub przeprowadza odpowiednie szkolenia.

3.4. Podczas wdrożenia dokumentów należy uwzględnić rotację Personelu.

4. Obowiązki wynikające z przepisów prawa

4.1. Administrator ma obowiązek stosować wszystkie adekwatne do jego działalności wymogi ochrony danych osobowych:

4.1.1. przestrzegania zasad przetwarzania danych osobowych określonych w art. 5 RODO,

4.1.2. przetwarzania danych osobowych wyłącznie w oparciu o podstawy prawne określone w art. 6, 9 i 10 RODO,

4.1.3. realizacji obowiązków informacyjnych zgodnie z art. 13 i 14 RODO,

4.1.4. umożliwienia osobom fizycznym realizacji praw wymienionych w art. 12-22 RODO,

4.1.5. wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie danych odbywało się zgodnie z przepisami RODO oraz aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw oraz wolności osób fizycznych (art. 24 i 32 RODO),

4.1.6. uwzględniania ochrony danych w fazie projektowania oraz stosowania domyślnej ochrony danych (art. 25 RODO),

4.1.7. dokonania pisemnych uzgodnień ze Współadministratorem (art. 26 RODO),

4.1.8. przestrzegania wymogów dotyczących powierzenia przetwarzania danych innemu podmiotowi określonych w art. 28 RODO, w tym w sytuacji, w której sam działa jako podmiot przetwarzający dane mu powierzone,

4.1.9. zapewnienia przetwarzania danych wyłącznie na polecenie Administratora przez podmioty przetwarzające oraz każdą osobę

działającą z upoważnienia Administratora lub podmiotu przetwarzającego, mającą dostęp do danych – chyba że wymaga tego prawo (art. 29 RODO),

4.1.10. prowadzenia rejestru czynności przetwarzania oraz – gdy ma to zastosowanie – rejestru kategorii czynności przetwarzania, zgodnie z art. 30 RODO,

4.1.11. zgłaszania naruszeń ochrony danych osobowych do UODO oraz w określonych przypadkach powiadamiania osób fizycznych o tych naruszeniach (art. 33 i 34 RODO),

4.1.12. wykonywania oceny skutków dla danych osobowych (art. 35 RODO),

4.1.13. przeprowadzania uprzednich konsultacji zgodnie z art. 36 RODO,

4.1.14. przestrzegania wymogów odnoszących się do przekazywania danych osobowych do państw trzecich (art. 44 – 49 RODO),

4.1.15. gdy ma to zastosowanie – wyznaczenia Inspektora Ochrony Danych (art. 37 RODO).

5. Zasady i podstawy prawne przetwarzania danych osobowych

5.1. Administrator zapewnia, że dane osobowe będą:

5.1.1. przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („**zgodność z prawem, rzetelność i przejrzystość**");

5.1.2. zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; **(„ograniczenie celu")**;

5.1.3. adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (**„minimalizacja danych"**);

5.1.4. prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane **(„prawidłowość");**

5.1.5. przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; **(„ograniczenie przechowywania");**

5.1.6. przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych **(„integralność i poufność").**

5.2. Administrator jest odpowiedzialny za przestrzeganie zasad przetwarzania danych osobowych i musi być w stanie wykazać ich przestrzeganie ("**rozliczalność**").

5.3. W celu właściwej realizacji powyższych zasad Administrator wdraża w szczególności:

5.3.1. odpowiednie środki prawne, techniczne i organizacyjne oraz

5.3.2. procedury, instrukcje lub inne wewnętrzne dokumenty regulujące przestrzeganie zasad przetwarzania danych osobowych lub

5.3.3. wewnętrzne materiały informacyjne i edukacyjne dla personelu przetwarzającego dane osobowe lub

5.3.4. szkolenia personelu przetwarzającego dane osobowe.

6. Podstawy prawne legalizujące przetwarzanie

6.1. Dopuszczalnymi przez przepisy podstawami legalizującymi przetwarzanie danych osobowych są:

6.1.1. zgoda osoby, której dane dotyczą,

6.1.2. niezbędność przetwarzania danych w celu wykonania umowy zawartej z osobą, której dane dotyczą, lub do podjęcia działań na żądanie tej osoby przed zawarciem umowy,

6.1.3. niezbędność przetwarzania danych w celu wypełnienia obowiązku prawnego ciążącego na Administratorze,

6.1.4. niezbędność przetwarzania danych w celu ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej,

6.1.5. niezbędność przetwarzania danych do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej,

6.1.6. niezbędność przetwarzania danych do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora lub 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.

6.2. Dopuszczalnymi przez przepisy podstawami legalizującymi przetwarzanie danych szczególnej kategorii są:

6.2.1. wyraźna zgoda osoby, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu przetwarzania danych szczególnej kategorii;

6.2.2. niezbędność przetwarzania danych w celu 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;

6.2.3. niezbędność przetwarzania danych w celu ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;

6.2.4. przetwarzanie jest dokonywane 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 danych dotyczy wyłącznie 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;

6.2.5. przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;

6.2.6. przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;

6.2.7. niezbędność przetwarzania danych 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;

6.2.8. niezbędność przetwarzania danych 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;

6.2.9. niezbędność przetwarzania danych 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;

6.2.10. niezbędność przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych 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.

6.3. Dopuszczalnymi przez przepisy podstawami legalizującymi przetwarzanie danych osobowych dotyczących wyroków skazujących oraz czynów zabronionych lub powiązanych z nimi środków bezpieczeństwa jest przetwarzanie danych na podstawie art. 6 ust. 1 RODO i jednocześnie: wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem Unii lub prawem

państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą.

6.4. W celu zapewnienia przetwarzania danych zgodnego z przepisami Administrator weryfikuje podstawy prawne dla każdej czynności przetwarzania danych oraz nie dopuszcza do przetwarzania danych, dla których nie ma legalnych podstaw.

7. Prawa osób, których dane dotyczą

7.1. Administrator jest zobowiązany do respektowania praw przyznanych osobom fizycznym przepisami RODO:

7.1.1. dostępu do danych,

7.1.2. sprostowania danych,

7.1.3. usunięcia danych,

7.1.4. ograniczenia przetwarzania,

7.1.5. obowiązku powiadomienia odbiorców o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania,

7.1.6. przenoszenia danych,

7.1.7. sprzeciwu wobec przetwarzania danych,

7.1.8. prawa do niepodlegania zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu,

7.2. Administrator jest zobowiązany do realizacji obowiązku informacyjnego zgodnie z art. 13 i 14 RODO, tj. przekazywania osobom, których dane dotyczą, następujących informacji:

7.2.1. Zgodnie z art. 13 RODO:

- 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 danych osobowych, oraz podstawę prawną przetwarzania,
- 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 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, art. 47 lub art. 49 ust. 1 akapit drugi RODO, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz informację o sposobach

uzyskania kopii tych zabezpieczeń lub o miejscu ich udostępnienia,

- okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
- informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,
- 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,
- informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych,
- 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;

7.2.2. Zgodnie z art. 14 RODO:

- 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, art. 47 lub art. 49 ust. 1 akapit drugi RODO, wzmiankę o

odpowiednich lub właściwych zabezpieczeniach oraz informację o sposobach uzyskania kopii tych zabezpieczeń lub o miejscu ich udostępnienia,

- 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.

7.3. Administrator jest zobowiązany do realizacji obowiązku informacyjnego w następujących terminach:

7.3.1. Zgodnie z art. 13 RODO:

- podczas pozyskiwania danych osobowych,

7.3.2. Zgodnie z art. 14 RODO:

- 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.

7.3.3. W celu właściwej realizacji praw osób, których dane dotyczą, Administrator wdraża procedury, instrukcje lub inne wewnętrzne dokumenty określające postępowanie w przypadku realizacji praw osób.

7.4. Ponadto Administrator wdraża środki organizacyjne oraz techniczne umożliwiające zarządzanie wyrażonymi zgodami na przetwarzanie danych osobowych, polegające na udokumentowaniu wyrażenia zgody oraz jej wycofania.

8. Ochrona danych osobowych w fazie projektowania oraz domyślna ochrona danych

8.1. Podczas planowania procesów, podczas których będzie dochodziło do przetwarzania danych osobowych, konieczne jest przeprowadzenie oceny w zakresie uwzględnienia wymogów ochrony danych osobowych wynikających z RODO.

8.2. Podczas oceny należy wziąć po uwagę:

- stan wiedzy technicznej,
- koszt wdrażania,
- charakter, zakres, kontekst i cele przetwarzania,
- ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania.

8.3. Proces może zostać uruchomiony tylko w przypadku spełnienia wymagań ochrony danych osobowych.

8.4. W celu uwzględnienia ochrony danych w fazie projektowania oraz stosowania domyślnej ochrony danych Administrator wdraża odpowiednie środki organizacyjne.

9. Współadministrowanie danymi osobowymi

9.1. W przypadku, gdy Administrator będzie wspólnie z innym podmiotem lub podmiotami ustalał cele i sposoby przetwarzania danych osobowych, konieczne jest dokonanie wspólnych uzgodnień pomiędzy podmiotami będącymi współadministratorami. Uzgodnienia takie mogą przyjąć formę w szczególności umowy lub innego porozumienia stron.

9.2. Uzgodnienia muszą określać odpowiednie zakresy odpowiedzialności współadministratorów dotyczącej wypełniania obowiązków wynikających z RODO, w szczególności w odniesieniu do realizacji praw osób oraz wypełnienia obowiązków informacyjnych, o których mowa w art. 13 i 14 RODO, chyba że przypadające współadministratorom obowiązki i ich zakres określa prawo Unii lub prawo państwa członkowskiego, któremu podlegają współadministratorzy. W uzgodnieniach należy także wskazać punkt kontaktowy dla osób, których dane dotyczą. Zasadnicza treść uzgodnień jest udostępniana podmiotom, których dane dotyczą.

9.3. W celu przestrzegania obowiązków dotyczących współadministrowania Administrator weryfikuje zasady współpracy z innymi podmiotami w zakresie ustalenia, czy dochodzi do współadministrowania danymi z innymi podmiotami.

10. Powierzenie przetwarzania danych osobowych

10.1. Administrator może powierzyć przetwarzanie danych osobowych wyłącznie podmiotom, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

10.2. W celu realizacji obowiązku, o którym jest mowa powyżej, Administrator wdraża odpowiednie środki organizacyjne, takie jak:

10.2.1. weryfikacja potencjalnego kontrahenta przez wysłanie ankiety z pytaniami dotyczącymi spełniania wymogów RODO lub

10.2.2. weryfikacja potencjalnego kontrahenta przez przeprowadzenie kontroli w zakresie wypełniania wymogów RODO. Kontrola ta może obejmować systemy, pomieszczenia i dokumentację przetwarzania danych osobowych kontrahenta.

10.3. W celu realizacji obowiązku, o którym mowa w pkt 10.1. powyżej, w szczególności w przypadku, gdy warunki współpracy mające wpływ na przetwarzanie danych osobowych przez kontrahenta ulegają zmianie lub w innych uzasadnionych przypadkach Administrator może ponownie przeprowadzić weryfikację wypełniania wymogów RODO przez tego kontrahenta, zgodnie z zawartymi umowami powierzenia przetwarzania danych.

10.4. Administrator powierza dane osobowe innemu podmiotowi w drodze umowy lub innego instrumentu prawnego zawartego w formie pisemnej lub elektronicznej.

10.5. Administrator w celu kontroli realizacji obowiązków wynikających z powierzenia danych osobowych wdraża odpowiednie środki organizacyjne, takie jak:

10.5.1. weryfikacja zasad współpracy z kontrahentami w zakresie powierzania danych osobowych,

10.5.2. rejestr podmiotów przetwarzających,

10.5.3. weryfikacja zgodności zawartych umów powierzenia z wymogami RODO.

11. Naruszenia ochrony danych osobowych

11.1. W przypadku naruszenia ochrony danych osobowych, Administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je do UODO, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego do UODO po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

11.2. Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby zapobiegać wystąpieniu naruszeń ochrony danych osobowych.

11.3. Administrator zapewnia, że:
    11.3.1. Personel został poinstruowany o sytuacjach, jakie można uznać za naruszenia ochrony danych,
    11.3.2. Personel został poinformowany o tym, jak należy postąpić w przypadku dostrzeżenia naruszenia ochrony danych osobowych,
    11.3.3. została wyznaczona osoba, która przyjmuje zgłoszenia o naruszeniach ochrony danych osobowych od Personelu,
    11.3.4. została wdrożona procedura postępowania w przypadku zaistnienia naruszenia ochrony danych osobowych,
    11.3.5. dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze w prowadzonym rejestrze naruszeń.
11.4. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

12. Inspektor ochrony danych

12.1. Gdy ma to zastosowanie, Administrator wyznacza inspektora ochrony danych, który podlega wyłącznie najwyższemu kierownictwu.
12.2. Administrator podejmuje działania, aby Inspektor ochrony danych:
    12.2.1. był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych,
    12.2.2. był włączany w wykonanie oceny skutków dla ochrony danych osobowych jeśli jest obowiązek dokonania takiej oceny,
    12.2.3. był punktem kontaktowym dla osób, których dane dotyczą,
    12.2.4. był punktem kontaktowym dla organu nadzorczego.
12.3. Inspektor ochrony danych nie może otrzymywać instrukcji dotyczących wykonywania swoich zadań oraz nie może być odwołany ani karany za wypełnianie swoich zadań.
12.4. Dane kontaktowe inspektora są publikowane na stronie internetowej Administratora oraz w klauzulach informacyjnych przekazywanych osobom, których dane są pozyskiwane. Jeśli Administrator nie prowadzi własnej strony internetowej, dane kontaktowe inspektora są udostępniane w sposób ogólnie dostępny w miejscu prowadzenia działalności.
12.5. Osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych i wykonywaniem praw przysługujących im na mocy RODO.
12.6. Inspektor ochrony danych jest zobowiązany do zachowania tajemnicy lub poufności wszelkich informacji pozyskanych bezpośrednio lub pośrednio w związku z wykonywaniem swoich zadań.
12.7. Zadania inspektora ochrony danych:

12.7.1. informowanie Administratora oraz członków personelu Administratora o obowiązkach spoczywających na nich na mocy przepisów o ochronie danych osobowych i doradzanie im w tej sprawie,

12.7.2. monitorowanie przestrzegania przepisów o ochronie danych osobowych oraz polityk i procedur przyjętych przez Administratora w tej dziedzinie,

12.7.3. podejmowanie działań zwiększających świadomość i szkolenia personelu Administratora uczestniczącego w operacjach przetwarzania danych,

12.7.4. prowadzenie audytów zgodności przetwarzania danych z przepisami,

12.7.5. udzielanie na żądanie Administratora zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania,

12.7.6. współpraca z Urzędem Ochrony Danych Osobowych,

12.7.7. pełnienie funkcji punktu kontaktowego dla Urzędu Ochrony Danych Osobowych w kwestiach związanych z przetwarzaniem oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach,

12.7.8. pełnienie funkcji punktu kontaktowego dla osób, których dane są przetwarzane przez Administratora.

13. Przekazywanie danych do państwa trzeciego lub organizacji międzynarodowej

13.1. Dane osobowe mogą być przekazywane do państwa trzeciego lub organizacji międzynarodowej tylko w przypadkach, gdy zostaną spełnione warunki określone w przepisach RODO, oraz zapewniając, że nie zostanie naruszony stopień ochrony osób fizycznych zagwarantowany w RODO.

13.2. Podstawami prawnymi umożliwiającymi przekazywanie danych do państw trzecich są:

13.2.1. decyzja Komisji Europejskiej stwierdzająca odpowiedni stopień ochrony w danym państwie trzecim, na danym terytorium lub w określonym sektorze w tym państwie lub danej organizacji międzynarodowej,

13.2.2. zapewnienie przez Administratora odpowiednich zabezpieczeń i obowiązywanie egzekwowalnych praw osób, których dane dotyczą, oraz skutecznych środków ochrony prawnej,

13.2.3. wyraźna zgoda osoby, której dane dotyczą, poinformowanej o ewentualnym ryzyku, z którym - ze względu na brak decyzji stwierdzającej odpowiedni stopień ochrony oraz na brak odpowiednich zabezpieczeń - może się dla niej wiązać proponowane przekazanie

13.2.4. niezbędność przekazania do wykonania umowy zawartej między osobą, której dane dotyczą, a Administratorem lub do wprowadzenia w życie środków przedumownych podejmowanych na żądanie osoby, której dane dotyczą,

13.2.5. niezbędność przekazania do zawarcia lub wykonania umowy zawartej w interesie osoby, której dane dotyczą, między Administratorem a inną osobą fizyczną lub prawną

13.2.6. niezbędność przekazania ze względu na ważne względy interesu publicznego,

13.2.7. niezbędność przekazania do ustalenia, dochodzenia lub ochrony roszczeń,

13.2.8. niezbędność przekazania do ochrony żywotnych interesów osoby, której dane dotyczą, lub innych osób, jeżeli osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody,

13.2.9. przekazanie następuje z rejestru, który zgodnie z prawem Unii lub prawem państwa członkowskiego ma służyć za źródło informacji dla ogółu obywateli i który jest dostępny dla ogółu obywateli lub dla każdej osoby mogącej wykazać prawnie uzasadniony interes – ale wyłącznie w zakresie, w jakim w danym przypadku spełnione zostały warunki takiego dostępu określone w prawie Unii lub w prawie państwa członkowskiego,

13.2.10. jeśli nie istnieje żadna z podstaw określonych powyżej – przekazanie do państwa trzeciego lub organizacji międzynarodowej może nastąpić wyłącznie, gdy przekazanie nie jest powtarzalne, dotyczy tylko ograniczonej liczby osób, których dane dotyczą, jest niezbędne ze względu na ważne prawnie uzasadnione interesy realizowane przez Administratora, wobec których charakteru nadrzędnego nie mają interesy ani prawa i wolności osoby, której dane dotyczą, a Administrator ocenił wszystkie okoliczności przekazania danych i na podstawie tej oceny zapewnił odpowiednie zabezpieczenia w zakresie ochrony danych osobowych. Administrator informuje organ nadzorczy o przekazaniu. Poza wypełnieniem klauzuli informacyjnej Administrator podaje osobie, której dane dotyczą, także informacje o przekazaniu i o ważnych prawnie uzasadnionych interesach realizowanych przez niego.

13.3. W przypadku, gdy dane będą miały być przekazywane do państwa trzeciego Administrator zapewnia:

13.3.1. przeprowadzenie analizy prawnej dotyczącej możliwości legalnego przekazywania danych,

13.3.2. przekazywanie danych wyłącznie na podstawie obowiązujących podstaw prawnych.

14. Środki techniczne i organizacyjne oraz analiza ryzyka naruszenia praw lub wolności osób fizycznych

14.1. Obowiązki Administratora w zakresie środków technicznych i organizacyjnych

14.1.1. Administrator uwzględniając:

- stan wiedzy technicznej,
- koszt wdrażania oraz
- charakter, zakres, kontekst i cele przetwarzania oraz
- ryzyko naruszenia praw lub wolności osób fizycznych

jest zobowiązany do :

- zapewnienia zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania danych osobowych,
- zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
- regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania,
- zdefiniowania i wdrożenia odpowiednich środków technicznych i organizacyjnych, zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku przetwarzania.

14.1.2. Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z:

- przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji,
- nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych

14.1.3. Metodyka szacowania ryzyka bezpieczeństwa danych osobowych została określona w punkcie 17. Polityki.

14.2. Podstawowe zasady bezpieczeństwa

14.2.1. Zarządzanie dostępem do obszarów przetwarzania danych osobowych

- Administrator projektuje i stosuje fizyczne zabezpieczenia przed dostępem osób nieuprawnionych do obiektów i pomieszczeń,
- Administrator zabezpiecza wewnętrzną sieć teleinformatyczną przed dostępem osób nieuprawnionych,
- Administrator opracowuje i wdraża dokumentację określającą zasady bezpieczeństwa, w szczególności:
  - ochrony fizycznej oraz zasady „czystego biurka",
  - zasady poruszania się gości,
  - niszczenia nośników danych osobowych,
  - monitoringu wizyjnego,
  - ochrony antywirusowej.

14.2.2. Inwentaryzacja sprzętu i oprogramowania informatycznego

- Administrator przygotowuje i utrzymuje aktualność spisu inwentaryzacyjnego sprzętu i oprogramowania informatycznego służącego do przetwarzania danych osobowych,
- Administrator opracowuje i wdraża dokumentację określającą odpowiednie zasady inwentaryzacji sprzętu i oprogramowania.

14.2.3. Zarządzanie dostępem do systemów

- Przyznawanie dostępu do systemów jest ograniczone i kontrolowane,
- Administrator opracowuje i wdraża dokumentację określającą zasady przyznawania dostępu do systemów.

14.2.4. Kryptografia

- W celu ochrony poufności Administrator stosuje techniki kryptograficzne, w szczególności szyfrowanie dysków urządzeń mobilnych oraz innych nośników, w trakcie przesyłania danych uwierzytelniających oraz danych osobowych, w przypadku przekazywania plików zawierających dane osobowe na nośnikach wymiennych,
- Administrator opracowuje i wdraża dokumentację określającą zasady stosowania kryptografii.

14.2.5. Urządzenia mobilne, praca zdalna i BYOD

- Administrator wdraża wymogi bezpieczeństwa dla urządzeń mobilnych przetwarzających dane osobowe,
- W przypadku występowania pracy zdalnej Administrator wdraża zasady wykonywania telepracy,
- Jeżeli do pracy wykorzystywane są urządzenia prywatne, Administrator wdraża minimalne wymogi zabezpieczenia, jakie powinny spełniać takie urządzenia,
- Administrator opracowuje i wdraża dokumentację określającą zasady bezpieczeństwa urządzeń mobilnych, pracy zdalnej i BYOD.

14.2.6. Kopie zapasowe i gwarantowanie zasilania

- Na potrzeby zachowania dostępności do danych Administrator zabezpiecza infrastrukturę teletechniczną przed brakiem zasilania oraz wykonuje kopie zapasowe danych osobowych,
- Administrator opracowuje i wdraża dokumentację określającą zasady gwarantowania zasilania oraz wykonywania kopii zapasowych dla poszczególnych systemów.

14.2.7. Audyty

- Administrator przeprowadza cykliczne audyty w celu sprawdzenia stopnia realizacji obowiązków wynikających z przepisów ochrony danych osobowych, ustalonej Polityki, przyjętych u Administratora wytycznych i standardów,

- Wyniki audytu stanowią podstawę do ustalenia działań, jakie należy podjąć celem dostosowania działalności Administratora do przepisów ochrony danych osobowych, ustalonej Polityki, przyjętych u Administratora wytycznych i standardów.

15. Ocena skutków dla ochrony danych osobowych (DPIA)

15.1. Jeżeli dany rodzaj przetwarzania - w szczególności z użyciem nowych technologii - ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.

15.2. Wykonanie oceny skutków dla ochrony danych osobowych jest obowiązkowe w szczególności w przypadku:

15.2.1. systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną,

15.2.2. przetwarzania na dużą skalę szczególnych kategorii danych osobowych, lub danych osobowych dotyczących wyroków skazujących i czynów niedozwolonych lub powiązanych środków bezpieczeństwa,

15.2.3. systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie,

15.2.4. operacji przetwarzania ujętych w wykazie rodzajów operacji opublikowanym przez UODO.

15.3. Dokonując oceny skutków Administrator konsultuje się z inspektorem ochrony danych, gdy ma to zastosowanie.

15.4. W stosownych przypadkach Administrator zasięga opinii osób, których dane dotyczą, lub ich przedstawicieli w sprawie zamierzonego przetwarzania, bez uszczerbku dla ochrony interesów handlowych lub publicznych lub bezpieczeństwa operacji przetwarzania.

15.5. W razie potrzeby, przynajmniej gdy zmienia się ryzyko wynikające z operacji przetwarzania, Administrator dokonuje przeglądu, by stwierdzić, czy przetwarzanie odbywa się zgodnie z oceną skutków dla ochrony danych.

15.6. Jeżeli ocena skutków dla ochrony danych wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby Administrator nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania Administrator konsultuje się z UODO.

15.7. Administrator opracowuje dokumentację oceny skutków dla ochrony danych, która zawiera co najmniej:

- opis planowanych operacji przetwarzania i celów przetwarzania,
- ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne,
- ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą,
- środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych.

16. Obowiązki dotyczące Personelu

16.1. Administrator opracowuje i wdraża dokumentację określającą szczegółowe obowiązki Personelu w zakresie przetwarzania danych osobowych.

16.2. Administrator zapewnia, że osoby mające dostęp do danych osobowych, przed dopuszczeniem ich do przetwarzania danych osobowych:

16.2.1. posiadają nadane upoważnienie do przetwarzania danych osobowych,

16.2.2. są szkolone z przetwarzania danych osobowych,

16.2.3. zapoznają się z dokumentacją określającą zasady przetwarzania danych osobowych,

16.2.4. pisemnie zobowiązują się do zachowania w tajemnicy danych osobowych oraz przetwarzania danych osobowych wyłącznie na polecenie Administratora.

16.3. Administrator prowadzi ewidencję osób upoważnionych.

17. Metodyka Zarządzania Ryzykiem

17.1. Wprowadzenie

17.1.1. Zgodnie z RODO, w tym motywem 76 RODO, Administrator zobowiązany jest ocenić „prawdopodobieństwo i powagę ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, należy określić poprzez odniesienie się do charakteru, zakresu, kontekstu i celów przetwarzania danych. Ryzyko należy oszacować na podstawie obiektywnej oceny, w ramach której stwierdza się, czy z operacjami przetwarzania danych wiąże się ryzyko lub wysokie ryzyko".

17.1.2. Metodyka opisuje: cele, proces zarządzania ryzykiem, metodykę wykonywania oceny ryzyka (w tym kryteria szacowania i akceptacji ryzyka), tak aby zapewnić bezpieczeństwo danych oraz zgodność z przepisami o ochronie danych osobowych. Podstawy funkcjonowania Metodyki opierają się na przepisach prawa oraz międzynarodowych normach, m.in.:

- RODO,
- Wytycznych Grupy Roboczej ds. Ochrony danych 29 14/EN WP 218 w sprawie oceny oddziaływania na ochronę danych i określenia czy przetwarzanie "może prowadzić do wysokiego ryzyka" w rozumieniu rozporządzenia 2016/679,
- Normy ISO/IEC 27001:2017,

- Normy ISO/IEC 29134:2017.

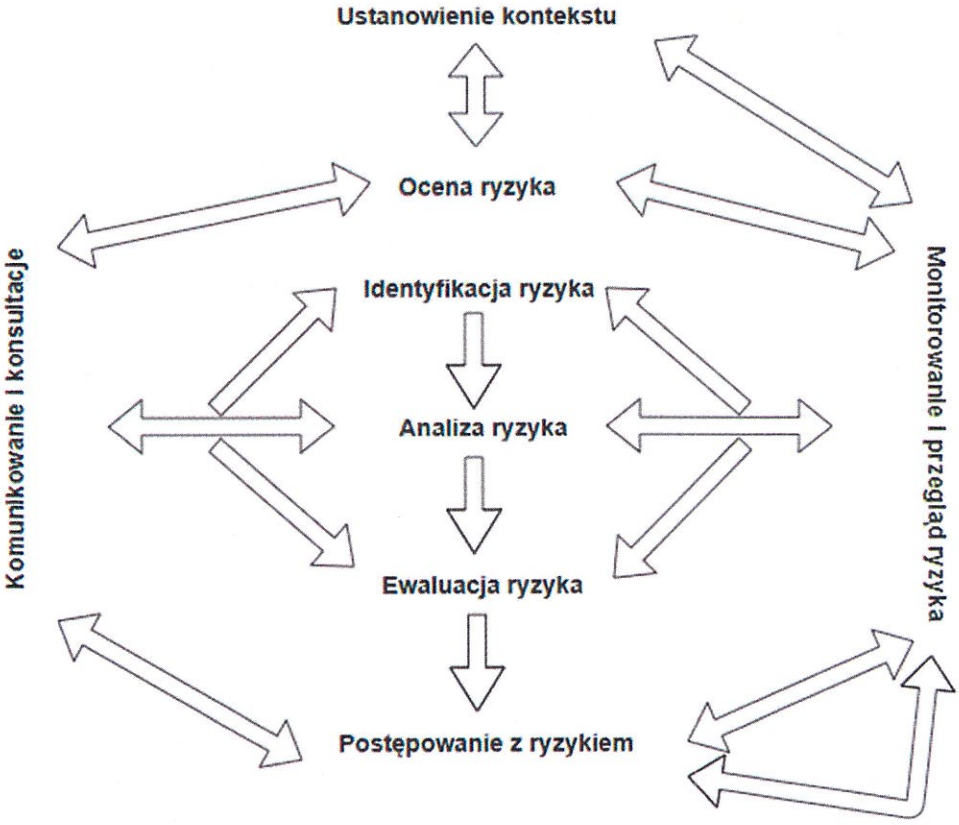
17.1.3. Celem Metodyki jest ustanowienie procesu zarządzania ryzykiem przez Administratora. Zarządzanie ryzykiem w ochronie danych osobowych ma za zadanie:

- zapewnienie zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
- definiowanie i wdrażanie odpowiednich środków technicznych i organizacyjnych, zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku;
- dokonanie oceny, czy stopień bezpieczeństwa jest odpowiedni, uwzględniając ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
- wypełnienie obowiązków zawartych w art. 24, 25, 32 oraz 35 RODO.

17.1.4. Zarządzanie ryzykiem jest procesem ciągłym, monitorującym adekwatność oraz skuteczność stosowanych zabezpieczeń organizacyjnych i technicznych, w celu utrzymania ryzyka na akceptowalnym poziomie. Stosowana przez Administratora metodyka zarządzania ryzykiem ma zapewnić porównywalne i powtarzalne rezultaty, poprzez zastosowanie standaryzacji skal oceny oraz sposobu przeprowadzania analizy, niezależnie od tego, kto i kiedy będzie przeprowadzał analizę i ocenę ryzyka danych osobowych w organizacji.

17.2. Proces zarządzania ryzykiem

17.2.1. Diagram przedstawiający proces zarządzania ryzykiem



17.3. Metodyka szacowania ryzyka bezpieczeństwa danych osobowych

17.3.1. Schemat procesu szacowania ryzyka

1	**Inwentaryzacja procesów i aktywów**
2	**Identyfikacja zagrożeń**
3	**Określenie podatności**
4	**Szacowanie ryzyka**
5	**Postępowanie z ryzykiem**

17.3.2. Opis procesu szacowania ryzyka.

- **Inwentaryzacja procesów i aktywów**
  Systematyczny opis operacji przetwarzania danych osobowych (charakter, zakres, kontekst i cele) oraz aktywów wraz z zabezpieczeniami wspierających procesy przetwarzania (w szczególności lokalizacje, hardware, software, sieci, personel).
- **Identyfikacja zagrożeń**
  Identyfikacja źródeł potencjalnych szkód dla praw i wolności osób fizycznych, w tym prawa do poufności, integralności oraz

dostępności danych osobowych (w oparciu o katalog zagrożeń zawartych w: ISO/IEC 27005:2018, NIST SP 800-30 – Guide for Conducting Risk Assessments).

- **Identyfikacje podatności**
  Identyfikacja słabości, które mogą być wykorzystane przez zagrożenia, powodując niekorzystne skutki. Dla każdego aktywu organizacji przypisany zostanie szereg zagrożeń oraz wskazane zostaną podatności, które pomogą ustalić realne słabości bezpieczeństwa danych osobowych organizacji.
- **Szacowanie ryzyka**
  Całościowy proces analizy i oceny ryzyka. Ocena niezbędności i proporcjonalności danych osobowych w poszczególnych procesach przetwarzania oraz określenie prawdopodobieństwa wystąpienia zdarzenia i wpływu podatności na procesy.
- **Postępowanie z ryzkiem**
  W przypadku zidentyfikowania ryzyk krytycznych i wysokich wskazanie działań mających na celu zminimalizowanie ryzyka do poziomu akceptowalnego.

17.4. Kryteria szacowania i akceptacji ryzyka:

17.4.1. Kryteria prawdopodobieństwa

P - prawdopodobieństwo	
1	zdarzenie prawie nieprawdopodobne
2	zdarzenie mało prawdopodobne,
3	zdarzenie wysoce prawdopodobne
4	zdarzenie niemal pewne

17.4.2. Kryteria skutków

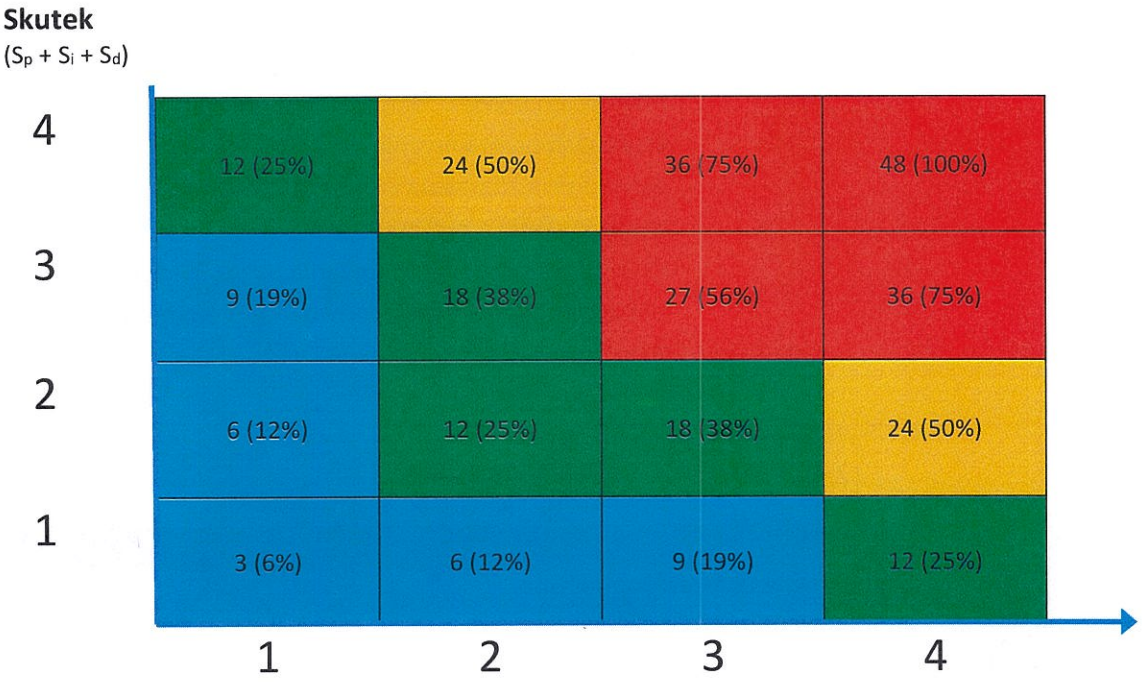
S – skutek dla poufności, integralności i dostępności (skutek dla bezpieczeństwa danych osobowych)	
1	zdarzenie wywołuje minimalny skutek,
2	zdarzenie wywołuje znaczący skutek,
3	zdarzenie wywołuje bardzo znaczący skutek,
4	zdarzenie wywołuje skutek katastrofalny,

17.4.3. Ocenę powagi ryzyka naruszenia bezpieczeństwa przetwarzania oblicza się na podstawie niniejszego wzoru:

$$R_p = P \times (S_p + S_i + S_d)$$

- gdzie:
  - R_p – poziom ryzyka,
  - P – wartość przypisana prawdopodobieństwu materializacji zagrożenia,
  - S_d – wartość przypisana skutkowi dla dostępności informacji,
  - S_i – wartość przypisana skutkowi dla integralności informacji,
  - S_p – wartość przypisana skutkowi dla poufności informacji,

17.4.4. Mapa ryzyka dla wzoru R = P x (S_p + S_i + S_d)



17.5. Metodyka szacowania skutków dla osób fizycznych

17.5.1. W przypadku zidentyfikowania wysokiego ryzyka podczas szacowania ryzyka bezpieczeństwa systemu danych osobowych dla procesu przetwarzania danych należy przeprowadzić ocenę skutków.

17.5.2. Do oceny skutków dla ochrony danych można wykorzystać taki sam schemat postępowania, jak dla szacowania ryzyka bezpieczeństwa danych osobowych, uwypuklając w poszczególnych etapach te elementy, które mają istotny wpływ na skutki, jakie naruszenie ochrony danych może powodować dla osób, których dane dotyczą.

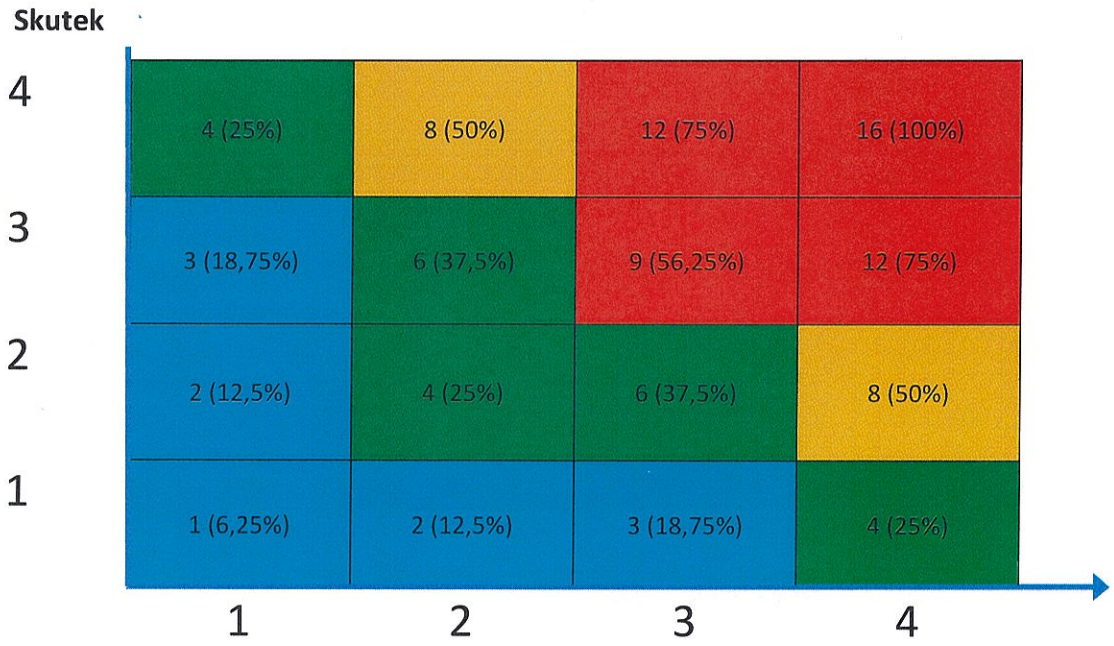
17.5.3. Ocena powagi ryzyka naruszenia praw i wolności osób oblicza się na podstawie niniejszego wzoru:

$$R_p = P \times S$$

- gdzie:

R_p – poziom ryzyka,
P – wartość przypisana prawdopodobieństwu materializacji zagrożenia,
S – wartość przypisana skutkowi dla osób fizycznych,

17.5.4. Mapa ryzyka dla wzoru R = P x S



17.5.5. Skutki dla osób fizycznych:

S – skutek dla osób fizycznych	
1	Wskazane skutki w kontekście urzeczywistnienia się analizowanego zagrożenia występują niezwykle rzadko. Podmioty danych nie zostaną dotknięte albo mogą napotkać nieliczne niedogodności, które przezwyciężą bez problemu (np. ponowne wprowadzanie danych/uzupełnianie, irytacja, rozdrażnienie itp.).
2	Identyfikuje się nieznaczne skutki mogące prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych dla osób fizycznych. Podmioty danych mogą napotkać istotne niedogodności, które będą w stanie przezwyciężyć mimo pewnych trudności (np. dodatkowe koszty, odmowa dostępu, stres, dolegliwości fizyczne).
3	Skutki mogą prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych dla osób fizycznych, jednakże nie są one wysokie. Podmioty danych mogą napotkać istotne skutki, które powinny być w stanie przezwyciężyć, choć z dużymi trudnościami (np. sprzeniewierzenie środków, uszkodzenie mienia, utrata pracy, pogorszenie stanu zdrowia itp.).
4	Skutki mogą prowadzić do wysokiego uszczerbku fizycznego, szkód majątkowych lub niemajątkowych dla osób fizycznych. Podmioty mogą napotkać istotne, a nawet nieodwracalne skutki, których mogą nie być w stanie przezwyciężyć (np. problemy finansowe, długotrwałe dolegliwości psychiczne lub fizyczne, zgon itp.).

17.5.6. Poziomy ryzyk dla bezpieczeństwa danych osobowych oraz oceny skutków:

Poziom ryzyka	Wartość dla $R = P \times (S_p + S_i + S_d)$	Wartość dla $R = P \times S$	Opis działania
Pomijalny	3-11 (6-23%)	1-3 (6-18%)	Poziom ryzyka akceptowalny – działania podejmowane w zależności od wymaganych nakładów.
Niski	12-18 (25-38%)	4-6 (25-38%)	Poziom ryzyka akceptowalny warunkowo – należy zminimalizować ryzyko jeżeli nie ma istotnych przeciwskazań, działanie może zostać przesunięte w czasie.
Średni	19-26 (40%-54%)	7-8 (44-50%)	Poziom ryzyka akceptowalny warunkowo **(S)** – działanie może zostać przesunięte w czasie, ale wymaga działań minimalizujących oraz monitorowania
Wysoki	27-48 (56%-100%)	9-16 (56-100%)	Poziom ryzyka nietolerowalny **(N)** – wymaga natychmiastowego działania konieczność przeprowadzenia oceny skutków (DPIA), należy rozważyć wstrzymanie procesu.

17.6. Postępowanie z ryzykiem

17.6.1. Celem postępowania z ryzykiem jest dokonanie wyboru sposobu postępowania z ryzykiem oraz zaplanowanie zabezpieczeń organizacyjnych i technicznych mających zapewnić minimalizację ryzyk oraz bezpieczeństwo danych osobowych.

17.6.2. W metodyce zostały przyjęte następujące warianty postępowania:

- minimalizacja ryzyka – wdrożenie adekwatnych zabezpieczeń technicznych i organizacyjnych mających na celu minimalizację ryzyka do poziomu akceptowalnego, a tym samym zapewnienie przestrzegania przepisów o ochronie danych osobowych;
- unikanie ryzyka – rezygnacja z realizacji działań lub warunków, które powodują powstanie określonych ryzyk;
- przeniesienie ryzyka - przeniesienie ryzyka na inny podmiot, który może skutecznie zarządzać ryzykiem;
- akceptacja ryzyka - podjęcie przez Administratora danych decyzji o zachowaniu ryzyka bez podejmowania dalszych działań.

17.6.3. Wynikiem szacowanego ryzyka w sytuacji opisanej w Art. 35 RODO będzie raport oceny skutków wraz z planem postępowania, który powinien uwzględniać:

- systematyczny opis planowanych operacji przetwarzania i celów przetwarzania (kontekst, zakres i cele przetwarzania);

- ocenę, czy operację przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
- ocenę ryzyka naruszenia praw i wolności osób (poziomy ryzyk dotyczących naruszenia praw lub wolności osób fizycznych);
- środki planowane w celu zaradzenia ryzyku - opis wariantu minimalizacji oraz działań jakie zostaną podjęte w celu minimalizacji ryzyka.

17.7. Monitorowanie i przegląd ryzyka

17.7.1. Monitorowanie i przegląd procesu szacowania ryzyka powinien być realizowany m.in., gdy:

a) zidentyfikowano nowy proces przetwarzania art. 25 RODO;
b) planowane są zmiany w obecnych procesach przetwarzania, np. wdrożenie nowej aplikacji/systemu przetwarzania, zmiana siedziby, migracja danych do chmury itp.;
c) organ nadzorczy ustanowił nowy lub zaktualizował wykaz rodzajów operacji przetwarzania podlegających i niepodlegających wymogowi przeprowadzenia oceny skutków dla ochrony danych;
d) zmieniły się lub planowane są zmiany warunków przyczyniających się do niezbędności i proporcjonalności przetwarzania danych;
e) zidentyfikowane ryzyka naruszenia praw lub wolności osób fizycznych są wciąż adekwatne;
f) zastosowane zabezpieczenia techniczne i organizacyjne są skuteczne i nadal minimalizują ryzyka.

17.7.2. Proces monitorowania powinien być realizowany na bieżąco w przypadkach wskazanych w pkt. 17.7.1. lit. a) – d) powyżej, natomiast przegląd określony w pkt. 17.7.1. lit. a) - f) powyżej powinien być przeprowadzony co najmniej raz w roku lub częściej.

17.7.3. Wyniki zarządzania ryzykiem będą dokumentowane w celu zachowania rozliczalności działań zgodnie z zasadą rozliczalności.

17.7.4. Przegląd powinien porównywać wyniki poprzednio przeprowadzonej analizy z kryteriami określonymi w pkt. 17.6.2 i 17.6.3. Polityki.

17.8. Konsultacje z organem nadzorczym

17.8.1. Jeżeli ocena skutków dla ochrony danych wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby Administrator nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania Administrator konsultuje się z organem nadzorczym.

17.8.2. Administrator konsultując się z organem nadzorczym zobowiązany jest przedstawić:

- Gdy ma to zastosowanie - odpowiednie obowiązki administratora, współadministratorów oraz podmiotów przetwarzających

uczestniczących w przetwarzaniu, w szczególności w przypadku przetwarzania w ramach grupy przedsiębiorstw;

- cele i sposoby zamierzonego przetwarzania danych;
- wykaz środków i zabezpieczeń mających chronić prawa i wolności osób, których dane dotyczą;
- dane kontaktowe inspektora ochrony danych – gdy ma to zastosowanie;
- ocenę skutków dla ochrony danych;
- wszelkie inne informacje, których żąda organ nadzorczy.

17.9. Role i odpowiedzialność

17.9.1. Za przeprowadzenie ogólnej analizy ryzyka i oceny skutków odpowiedzialny jest administrator danych.

17.9.2. Macierz odpowiedzialności za przeprowadzenie ogólnej analizy ryzyka i oceny skutków została opisana poniżej.

		Rola i odpowiedzialność			
Krok	Działanie	ADO	IOD	WP	E
1	Inwentaryzacja procesów i aktywów	A	C	R	R
2	Ocena, czy rodzaj operacji przetwarzania danych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych	A	R		R
3	Ocena, czy rodzaj operacji przetwarzania danych zwolniony jest z przeprowadzenia oceny skutków dla danych osobowych	A	R		R
4	Szacowanie ryzyka bezpieczeństwa danych osobowych	A	R	R	R
5	Szacowanie ryzyka naruszenia praw i wolności osób fizycznych	A	R	I	R
6	Przeprowadzenie postępowania z ryzykiem	A	R	R	R
7	Monitorowanie i przegląd ryzyka	A	R	R	R

ADO	Administrator danych
IOD	Inspektor danych osobowych lub osoba odpowiedzialna za ochronę danych osobowych
WP	Właściciel procesu
E	Eksperci

Responsible/Realizator	R	Osoba odpowiedzialna za realizację zadań
Accountable/Nadzór	A	Osoba nadzorująca i zatwierdzająca, odpowiedzialna za końcowy efekt zadań
Consulted/Doradztwo	C	Osoba konsultująca i doradzająca w realizacji zadań
Informed/Poinformowany	I	Osoba informowana o prowadzonych działaniach oraz niewpływająca na realizację zadań

Konwent Ojców **Bonifratrów**
Konary, ul. Bonifraterska **11**
32-031 **Mogilany**
Nip: **679-22-11-625**

PRZEOR
KONWENTU BONIFRTATRÓW
p. w. św. Józefa w Konarach
br. Anzelm Adam Skiba