POLITYKA OCHRONY DANYCH OSOBOWYCH

Międzynarodowe Stowarzyszenie Studentów Medycyny IFMSA-Poland

ul. Oczki 1A

02-007 Warszawa

Data wprowadzenia:	01/12/2021
Wersja:	1

SPIS TREŚCI

A. INFORMACJE OGÓLNE

1. CEL POLITYKI OCHRONY DANYCH OSOBOWYCH

Polityka ochrony danych osobowych została opracowana i wdrożona w strukturze Administratora Danych w celu zapewnienia zgodności przetwarzania danych osobowych z wymogami obowiązujących w tym zakresie polskich i europejskich aktów prawnych, w szczególności:

1. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),
2. Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r., poz. 1000 ze zm.).

Polityka ochrony danych osobowych ma zastosowanie do wszystkich pracowników Administratora Danych, którzy w zakresie swoich obowiązków służbowych przetwarzają dane osobowe, jak również innych osób, które z upoważnienia Administratora Danych uzyskały dostęp do danych osobowych. Każda z tych osób została zapoznana z najważniejszymi procedurami bezpieczeństwa danych opisanymi w Polityce ochrony danych osobowych i zobowiązana do ich przestrzegania w zakresie wynikającym z przydzielonych zadań. Osoby, o których mowa złożyły oświadczenie o zapoznaniu się z procedurami bezpieczeństwa danych oraz zobowiązały się do ich stosowania.

Wszelkie wątpliwości dotyczące sposobu interpretacji zapisów Polityki ochrony danych osobowych, powinny być rozstrzygane na korzyść zapewnienia możliwie najwyższego poziomu ochrony danych osobowych oraz realizacji praw osób, których dane dotyczą.

2. TERMINOLOGIA

1. **Administrator Danych** – Międzynarodowe Stowarzyszenie Studentów Medycyny IFMSA-Poland, ul. Oczki 1A, 02-007 Warszawa
2. **Administrator Systemów Informatycznych** lub **ASI** – osoba wyznaczona przez Administratora Danych, koordynująca działania związane z zapewnieniem bezpieczeństwa systemów informatycznych, w tym również odpowiadająca za nadzór nad zabezpieczeniem danych osobowych przetwarzanych w systemach informatycznych wykorzystywanych przez Administratora Danych,
3. **dane osobowe** – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"), gdzie poprzez możliwą do zidentyfikowania osobę fizyczną rozumie się osobę, 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,
4. **DPIA** – ocena skutków dla ochrony danych osobowych (*data protection impact assessment*),
5. **Oficer Bezpieczeństwa Danych Osobowych** lub **OBDO** – osoba wyznaczona przez Administratora Danych, koordynująca procesy związane z przestrzeganiem zasad ochrony danych osobowych w ramach procesów przetwarzania danych osobowych zachodzących w strukturze Administratora Danych,
6. **organ nadzorczy** – niezależny organ publiczny powołany w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych osobowych w Unii, powołany w każdym państwie członkowskim Unii, którego podstawowym zadaniem jest monitorowanie stosowania RODO,
7. **państwo trzecie** – państwo nienależące do Europejskiego Obszaru Gospodarczego.
8. **podmiot przetwarzający** –osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora Danych,
9. **Polityka** – niniejsza Polityka ochrony danych osobowych,
10. **pracownik** – osoba współpracująca z Administratorem Danych na podstawie umowy o pracę lub umowy cywilnoprawnej, każdy Członek Stowarzyszenia pełniący jakąkolwiek funkcję w strukturze organizacyjnej Administratora Danych,
11. **przetwarzanie** – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie 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,
12. **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 (ogólne rozporządzenie o ochronie danych),
13. **Unia** – Unia Europejska,

14. **Ustawa** – Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r., poz. 1000 ze zm.).

3. ZAKRES INFORMACJI OBJĘTYCH POLITYKĄ OCHRONY DANYCH OSOBOWYCH ORAZ ZAKRES ZASTOSOWANIA

Polityka ochrony danych osobowych opisuje zasady i procedury przetwarzania danych osobowych. Jest to zestaw praw, reguł i praktycznych doświadczeń dotyczących sposobu zarządzania, ochrony i dystrybucji danych osobowych wewnątrz Administratora Danych. Polityka ochrony danych osobowych odnosi się całościowo do problemu zabezpieczenia danych osobowych, tj. zarówno do zabezpieczenia danych przetwarzanych tradycyjnie, jak i danych przetwarzanych w systemach informatycznych.

Politykę ochrony danych osobowych stosuje się do wszelkich czynności, stanowiących w myśl RODO, przetwarzanie danych osobowych. Bez względu na źródło pochodzenia danych osobowych, ich zakres, cel zebrania, sposób przetwarzania lub czas przetwarzania, stosowane są zasady ujęte w Polityce.

Rygorowi Polityki podlegają także dane powierzone Administratorowi Danych do przetwarzania na podstawie umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego oraz dane osobowe, które zostały Administratorowi Danych udostępnione.

B. OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH

1. STRUKTURA ORGANIZACJI OCHRONY DANYCH OSOBOWYCH

Za przetwarzanie danych osobowych oraz ich ochronę zgodnie z postanowieniami RODO, Ustawy, Polityki oraz procedur wewnętrznych z zakresu ochrony danych osobowych wdrożonych w strukturze Administratora Danych, odpowiadają:

1. Administrator Danych,
2. Oficer Bezpieczeństwa Danych Osobowych,
3. Administrator Systemów Informatycznych,
4. Osoby zarządzające procesami przetwarzania danych osobowych,
5. Osoby upoważnione do przetwarzania danych osobowych.

1.1. ADMINISTRATOR DANYCH

1. Administrator Danych wyznacza:
   - 1.1. OBDO,
   - 1.2. ASI,
2. Administrator Danych jest odpowiedzialny za:
   - 2.1. zapewnienie odpowiednich środków organizacyjnych i technicznych w celu zapewnienia i wykazania przetwarzania danych osobowych zgodnie z zasadami przetwarzania danych osobowych określonymi w RODO,
   - 2.2. wdrożenie procedur ochrony danych osobowych,
   - 2.3. jeśli uzna to za konieczne, stosowanie zatwierdzonych kodeksów postępowania lub zatwierdzonych mechanizmów certyfikacji, jako element dla stwierdzenia przestrzegania przez Administratora Danych ciążących na nim obowiązków,
   - 2.4. zapewnienie środków umożliwiających prawidłową realizację praw osób, których dane dotyczą,
   - 2.5. współpracę z organem nadzorczym w ramach wykonywania przez niego swoich zadań,
   - 2.6. wdrożenie odpowiednich środków organizacyjnych i technicznych, aby zapewnić stopień bezpieczeństwa odpowiadający istniejącemu ryzyku naruszenia praw lub wolności osób, których dane dotyczą,
   - 2.7. zgłaszanie naruszenia ochrony danych osobowych właściwemu organowi nadzorczemu, a w przypadku, gdy zajdą ku temu odpowiednie przesłanki, również osobie, której dane dotyczą,

2.8. zapewnienie odpowiednich środków w celu dokonania oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych w sytuacji, jeżeli dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, w tym, jeżeli zajdą ku temu odpowiednie przesłanki, konsultacje z organem nadzorczym,

2.9. zapewnienie legalności przekazywania danych osobowych do podmiotów trzecich,

2.10. w stosunku do OBDO:

2.10.1. zapewnienie, że jest on właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych,

2.10.2. wspieranie OBDO w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej,

2.10.3. zagwarantowanie by OBDO nie działał pod wpływem presji i nie otrzymywał instrukcji dotyczących wykonywania swoich zadań,

3. Administrator Danych nadzoruje działania OBDO oraz ASI oraz wydaje im zalecenia, co do sposobu wykonywania obowiązków wynikających z Polityki.

4. Administrator Danych każdorazowo wyraża zgodę oraz ostateczną akceptację na kluczowe z perspektywy organizacji działania OBDO oraz ASI, w które zaangażowane są podmioty trzecie. Do zaakceptowania tych działań, wystarczająca jest zgoda wyrażona w formie wiadomości e-mail.

1.2. OFICER BEZPIECZEŃSTWA DANYCH OSOBOWYCH

1. Funkcję OBDO pełni osoba wyznaczona przez Administratora Danych.

2. Wzory dokumentów wyznaczenia oraz odwołania OBDO znajdują się w Załączniku nr 14 do Polityki.

3. OBDO jest wyznaczany przez Administratora Danych na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia swoich zadań.

4. Do zadań OBDO należy:

4.1. informowanie o obowiązkach wynikających z RODO oraz innych właściwych przepisów Unii lub państw członkowskich o ochronie danych osobowych oraz doradzanie w tym zakresie,

4.2. monitorowanie przestrzegania RODO oraz innych właściwych przepisów Unii lub państw członkowskich o ochronie danych osobowych,

4.3. monitorowanie przestrzegania wdrożonych procedur ochrony danych osobowych,

4.4. doradztwo w zakresie podziału obowiązków (np. między współadministratorami, Administratorem Danych a podmiotem przetwarzającym lub pomiędzy pracownikami Administratora Danych),

4.5. działania zwiększające świadomość pracowników Administratora Danych w zakresie obowiązków wynikających z RODO lub przyjętych procedur,

4.6. szkolenia dla pracowników Administratora Danych uczestniczących w operacjach przetwarzania danych,

4.7. przeprowadzanie audytów w zakresie przestrzegania RODO i wdrożonych procedur ochrony danych osobowych,

4.8. udzielanie na żądanie zaleceń, co do oceny skutków dla ochrony danych osobowych oraz monitorowanie jej wykonania / koordynowanie procesu oceny skutków dla ochrony danych osobowych,

4.9. współpraca z organem nadzorczym oraz pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych,

4.10. pełnienie funkcji punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO,

4.11. opracowywanie i aktualizacja Polityki, w tym podpisywanie zmodyfikowanych załączników do Polityki oraz ich wdrażanie, w przypadku zaistnienia zmian w Polityce, po jej pierwotnym wdrożeniu przez Administratora Danych,

4.12. administrowanie oraz kontrola upoważnień do przetwarzania danych osobowych,

4.13. udział w procesach związanych z naruszeniami ochrony danych osobowych, tj.:

4.13.1. prowadzenie rejestru naruszeń,

4.13.2. koordynowanie postępowania w sytuacji wykrycia naruszenia (dokumentacja naruszenia, postępowania naprawcze),

4.13.3. koordynowanie zgłoszenia naruszenia organowi nadzorczemu oraz osobom, których dane dotyczą,

4.14. opracowywanie unikalnych treści klauzul informacyjnych, klauzul zgód na przetwarzanie danych osobowych, umów powierzenia przetwarzania danych osobowych oraz innych klauzul / postanowień związanych z przetwarzaniem danych osobowych (np. postanowień w zakresie współadministrowania),

4.15. prowadzenie rejestru czynności przetwarzania danych osobowych,

4.16. prowadzenie rejestru kategorii czynności przetwarzania dokonywanych w imieniu innego administratora,

4.17. udział w procesie realizacji praw osób, których dane dotyczą (tj. udzielanie odpowiedzi na zapytania, prowadzenie korespondencji, spotkania z osobami realizującymi swoje prawa),

4.18. reagowanie na skargi osób, których dane dotyczą (tj. korespondencja z organem nadzorczym, korespondencja ze skarżącym),

4.19. udział w postępowaniach administracyjnych oraz sądowych prowadzonych w związku ze skargami osób, których dane dotyczą,

4.20. udział w procesach certyfikacji oraz przystępowania do funkcjonujących kodeksów postępowania,

4.21. kontrola podmiotów przetwarzających.

1.3. ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH

1. Funkcję ASI pełni osoba wyznaczona przez Administratora Danych.
2. Wzory dokumentów wyznaczenia oraz odwołania ASI znajdują się w Załączniku nr 15 do Polityki.
3. Do zadań ASI należy:
   - 3.1. prowadzenie rejestru nadanych uprawnień do systemów informatycznych,
   - 3.2. opracowywanie oraz aktualizacja Załącznika nr 13 do Polityki, który stanowi ogólny opis technicznych środków bezpieczeństwa wdrożonych w strukturze Administratora Danych,
   - 3.3. nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów,
   - 3.4. podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń,
   - 3.5. identyfikacja i analiza zagrożeń oraz ocena ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych,
   - 3.6. sprawowanie nadzoru nad kopiami zapasowymi,
   - 3.7. inicjowanie i nadzór nad wdrażaniem nowych narzędzi, procedur organizacyjnych oraz sposobów zarządzania systemami informatycznymi, które mają doprowadzić do wzmocnienia bezpieczeństwa przy przetwarzaniu danych osobowych,
   - 3.8. podejmowanie innych czynności w zakresie zabezpieczenia przetwarzania danych w systemach informatycznych,
   - 3.9. dokonywanie cyklicznych przeglądów aktualności i stosowania procedur z zakresu przetwarzania danych w systemach informatycznych, na podstawie opracowanego planu przeglądów,
   - 3.10. ścisła współpraca z OBDO w zakresie bezpieczeństwa i zasad przetwarzania danych osobowych w systemach informatycznych.

1.4. OSOBY ZARZĄDZAJĄCE PROCESAMI PRZETWARZANIA DANYCH OSOBOWYCH

1. Osobami zarządzającymi procesami przetwarzania danych osobowych są pracownicy Administratora Danych, którzy odpowiadają za bieżące zarządzanie procesami przetwarzania danych osobowych zachodzącymi w ramach funkcjonujących w strukturze Administratora Danych zbiorów danych.
2. Osoby zarządzające procesami przetwarzania danych osobowych są wskazywane przez Administratora Danych.

3. Dla każdego procesu przetwarzania danych osobowych musi zostać wyznaczona jedna osoba pełniąca obowiązki Osoby zarządzającej procesami przetwarzania danych osobowych, przy czym możliwe jest pełnienie tej funkcji przez jedną osobę w stosunku do kilku procesów przetwarzania danych osobowych.

4. Osoba zarządzająca procesami przetwarzania danych osobowych jest zobowiązana do ścisłej współpracy z OBDO w zakresie przetwarzania danych osobowych w zarządzanym przez nią procesie, a w szczególności zobowiązana jest do wykonywania jego poleceń w dziedzinie bezpieczeństwa przetwarzania danych osobowych.

5. Stosowny wykaz osób, które zostały wyznaczone do pełnienia funkcji Osoby zarządzającej procesami przetwarzania danych osobowych znajduje się w Załączniku nr 1 do Polityki.

6. Do uprawnień i obowiązków Osoby zarządzającej procesami przetwarzania danych osobowych należą, w szczególności:

   5.1. zgłaszanie do OBDO zamiaru wprowadzenia w zarządzanym przez nią procesie zmian w zakresie: sposobu zbierania oraz udostępniania danych, celu i zakresu przetwarzania danych, miejsca przetwarzania danych, zmiany formy przetwarzania danych, zaprzestania przetwarzania, usunięcia danych oraz zastosowanych zabezpieczeń związanych z przetwarzaniem,

   5.2. informowanie OBDO o planowanym wdrożeniu nowej operacji przetwarzania danych osobowych oraz planowanych zmianach w trwającej operacji przetwarzania, wobec której to operacji, istnieje prawdopodobieństwo obowiązku przeprowadzenia DPIA,

   5.3. udzielanie OBDO oraz innym pracownikom upoważnionym do przetwarzania danych osobowych wyjaśnień w sprawie zarządzanych przez nią procesów,

   5.4. nadzór nad wdrożeniem i stosowaniem fizycznych środków zabezpieczenia obszarów, w których przetwarzane są dane osobowe zawarte w procesie, którym zarządza.

6. W przypadku zmiany stanowiska pracy lub długotrwałej przerwy w jej wykonywaniu przez osobę pełniącą funkcję Osoby zarządzającej procesami przetwarzania danych osobowych należy dokonać wskazania innej osoby na jej miejsce.

7. Poprzez zmianę stanowiska pracy należy rozumieć zmianę stanowiska pracy w strukturze Administratora Danych jak i całkowite rozwiązanie stosunku pracy. Poprzez długotrwałą przerwę w wykonywaniu pracy należy rozumieć przerwę trwającą powyżej 30 dni.

1.5. OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Każda osoba, która uzyskała upoważnienie do przetwarzania danych, zobowiązana jest do ich ochrony w sposób zgodny z przepisami RODO, Ustawy oraz postanowieniami Polityki.

2. Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia. Stosowny zapis o przyjęciu zobowiązania do zachowania w tajemnicy przetwarzanych danych osobowych zawiera upoważnienie, którego wzór znajduje się w Załączniku nr 3 do Polityki.

3. Naruszenie obowiązku ochrony danych osobowych, a w szczególności obowiązku zachowania danych osobowych w tajemnicy skutkuje poniesieniem odpowiedzialności karnej na podstawie przepisów Ustawy oraz stanowi ciężkie naruszenie obowiązków pracowniczych i może być podstawą rozwiązania stosunku pracy w trybie art. 52 Ustawy z dnia 26 czerwca 1974 r. Kodeks Pracy (tekst jedn. Dz.U. z 2018 r., poz. 108 ze zm.), bądź rozwiązania stosunku cywilnoprawnego.

C. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

1. OGÓLNE ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

1. Przetwarzanie danych osobowych w strukturze Administratora Danych odbywa się zgodnie z ogólnymi zasadami przetwarzania danych osobowych określonymi w art. 5 RODO. Oznacza to, że dane osobowe przetwarza się:

   1.1 zgodnie z prawem, w oparciu o co najmniej jedną przesłankę legalności przetwarzania danych osobowych wskazaną w art. 6 lub 9 RODO (*zasada legalności*),

   1.2 w sposób rzetelny przy uwzględnieniu interesów i rozsądnych oczekiwań osób, których dane dotyczą (*zasada rzetelności*),

   1.3 w sposób przejrzysty dla osób, których dane dotyczą (*zasada przejrzystości*),

   1.4 w konkretnych, wyraźnych i prawnie uzasadnionych celach (*zasada ograniczenia celu*),

   1.5 w zakresie adekwatnym, stosownym oraz niezbędnym dla celów, w których są przetwarzane (*zasada minimalizacji danych*),

   1.6 przy uwzględnieniu ich prawidłowości i ewentualnego uaktualniania (*zasada prawidłowości*),

   1.7 przez okres nie dłuższy, niż jest to niezbędne dla celów, w których są przetwarzane (*zasada ograniczenia przechowywania*),

   1.8 w sposób zapewniający odpowiednie bezpieczeństwo (*integralność i poufność*).

2. Administrator Danych gwarantuje, że określone decyzje odnoszące się do procesów przetwarzania danych osobowych zostały przeanalizowane z punktu widzenia zgodności z ogólnymi zasadami przetwarzania danych, a przede wszystkim, że są z nimi zgodne.

2. ZAKRES PRZETWARZANYCH DANYCH OSOBOWYCH

1. Polityka ma zastosowanie w stosunku do wszystkich danych osobowych przetwarzanych przez Administratora Danych, niezależnie od formy ich przetwarzania (elektroniczna lub papierowa) oraz tego, czy są to dane przetwarzane w zbiorach danych, w zestawach czy stanowią one pojedyncze informacje osobowe.
2. Wykaz zbiorów danych osobowych, których administratorem jest Administrator Danych oraz procesów przetwarzania zachodzących w tych zbiorach stanowi Załącznik nr 1 do Polityki.
3. Administrator Danych we współpracy z OBDO prowadzi:
   - 3.1. rejestr czynności przetwarzania danych osobowych, których jest administratorem,
   - 3.2. rejestr kategorii czynności przetwarzania dokonywanych w imieniu administratorów, którzy powierzyli mu przetwarzanie danych.
4. Rejestr, o którym mowa w pkt 3.1. zawiera co najmniej następujące informacje:
   - 4.1. nazwę oraz dane kontaktowe Administratora Danych oraz wszelkich współadministratorów,
   - 4.2. gdy ma to zastosowanie imię, nazwisko lub nazwę oraz dane kontaktowe swojego przedstawiciela,
   - 4.3. imię i nazwisko oraz dane kontaktowe OBDO,
   - 4.4. cele przetwarzania,
   - 4.5. opis kategorii osób, których dane dotyczą,
   - 4.6. opis kategorii danych osobowych,
   - 4.7. kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych,
   - 4.8. gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń,
   - 4.9. jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,
   - 4.10. ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.
5. Rejestr, o którym mowa w pkt 3.2. zawiera co najmniej następujące informacje:
   - 5.1. nazwę oraz dane kontaktowe Administratora Danych,
   - 5.2. imię i nazwisko lub nazwę oraz dane kontaktowe każdego administratora, w imieniu którego działa Administrator Danych,
   - 5.3. gdy ma to zastosowanie, imię, nazwisko lub nazwę oraz dane kontaktowe przedstawiciela każdego administratora, w imieniu którego działa Administrator Danych,

5.4. gdy ma to zastosowanie, imię i nazwisko oraz dane kontaktowe OBDO lub IOD każdego administratora, w imieniu którego działa Administrator Danych,

5.5. kategorie przetwarzań dokonywanych w imieniu każdego z administratorów,

5.6. gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń,

5.7. ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

6. Administrator Danych we współpracy z OBDO prowadzi rejestry, o których mowa w pkt 3 w formie pisemnej, w tym elektronicznej.

7. W przypadku zgłoszenia przez organ nadzorczy żądania w tym zakresie, Administrator Danych udostępnia mu prowadzone przez siebie rejestry.

3. DOPUSZCZENIE OSÓB DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator Danych realizując Politykę, w zakresie udostępniania danych osobowych w ramach własnej (wewnętrznej) struktury, zezwala na ich przetwarzanie w systemie informatycznym lub w wersji papierowej wyłącznie osobom, które uzyskały uprzednie, stosowne upoważnienie do przetwarzania danych osobowych.
2. Upoważnienie do przetwarzania danych osobowych nadawane jest po przeprowadzeniu szkolenia lub zaznajomieniu w innej formie, osoby upoważnianej z zasadami ochrony danych osobowych obowiązującymi w strukturze Administratora Danych.
3. Upoważnienie do przetwarzania danych osobowych, nadawane jest indywidualnie, z wyraźnym wskazaniem, jakie zbiory danych obejmuje swoim zakresem.
4. OBDO prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, której wzór stanowi Załącznik nr 4 do Polityki.
5. Szczegółowa Procedura szkoleń oraz nadawania upoważnień do przetwarzania danych osobowych stanowi Załącznik nr 3 do Polityki.

4. POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator Danych realizując Politykę dopuszcza, by dane osobowe, których jest administratorem były przetwarzane poza własnymi strukturami organizacyjnymi. Może się to odbywać wyłącznie na drodze powierzenia danych, w określonym celu i zakresie, podmiotowi przetwarzającemu na mocy umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego.
2. Podstawowym warunkiem dopuszczalności powierzenia przetwarzania danych w imieniu administratora jest poddanie planowanego outsourcingu analizie, która powinna zapewnić, że wybór podmiotu przetwarzającego został uzależniony od zapewnienia wystarczających gwarancji ochrony danych.
3. Zawierana przez Administratora Danych umowa powierzenia przetwarzania danych osobowych musi być zgodna z postanowieniami art. 28 RODO, tj. w szczególności określać:
   - 3.1. przedmiot powierzenia,
   - 3.2. czas trwania powierzenia,
   - 3.3. charakter i cel przetwarzania,
   - 3.4. rodzaj powierzanych danych osobowych,
   - 3.5. kategorie osób, których dane dotyczą,
   - 3.6. warunki podpowierzenia przetwarzania danych
   - 3.7. obowiązki i prawa Administratora Danych,
   - 3.8. obowiązki podmiotu przetwarzającego.
4. Umowa powierzenia może zostać zawarta w formie pisemnej, w tym w elektronicznej.
5. W przypadku, gdy elementy powierzenia przetwarzania danych wskazane w pkt 3 znajdują się już w zawartej z danym podmiotem umowie, nie ma konieczności sporządzania dodatkowej umowy powierzenia przetwarzania danych osobowych.
6. Osoba zarządzająca procesami przetwarzania danych osobowych, przed planowanym rozpoczęciem współpracy z podmiotem przetwarzającym, jest zobowiązana poinformować o tym OBDO oraz skonsultować z nim postanowienia zawieranej umowy w zakresie powierzenia przetwarzania danych osobowych. Powierzenie przetwarzania danych może odbyć się wyłącznie na podstawie postanowień zaakceptowanych przez OBDO.
7. Umowa powierzenia przetwarzania danych osobowych podpisywana jest zgodnie z zasadami reprezentacji Administratora Danych lub udzielonymi pełnomocnictwami.
8. Każdorazowe dokonanie powierzenia danych osobowych musi zostać obligatoryjnie odnotowane w rejestrze czynności przetwarzania danych osobowych.
9. Administrator Danych ma prawo kontroli podmiotów przetwarzających, którym powierzył przetwarzanie danych osobowych. Procedura kontroli podmiotów przetwarzających stanowi Załącznik nr 11 do Polityki.
10. Administrator Danych w zakresie prowadzonej przez siebie działalności może przetwarzać również dane osobowe powierzone przez podmioty, na rzecz których świadczy usługi. Przyjęcie danych w powierzenie

przez Administratora Danych musi zostać obligatoryjnie odnotowane w rejestrze kategorii czynności przetwarzania danych osobowych.

5. UDOSTĘPNIENIE DANYCH OSOBOWYCH

1. Administrator Danych realizując Politykę dopuszcza, by dane osobowe, których jest administratorem były przekazywane innym administratorom w formie udostępnienia danych.
2. Udostępnienie danych osobowych może nastąpić tylko w oparciu o co najmniej jedną przesłankę spośród wskazanych w art. 6 RODO i / lub art. 9 RODO.
3. Podmioty lub kategorie podmiotów, którym udostępnia się dane osobowe muszą zostać obligatoryjnie wskazane w rejestrze czynności przetwarzania danych osobowych.

6. PRZEKAZYWANIE DANYCH OSOBOWYCH DO PAŃSTW TRZECICH

1. Przekazywanie danych, których administratorem jest Administrator Danych do państw trzecich i organizacji międzynarodowych, może się odbywać wyłącznie po spełnieniu warunków przewidzianych w Rozdziale V RODO.

2. Przekazywanie danych do państw trzecich może mieć formę zarówno powierzenia przetwarzania danych osobowych oraz udostępnienia danych osobowych, co oznacza, że w zależności od rodzaju przekazania, należy wziąć również pod uwagę postanowienia podrozdziałów 4 i 5 Polityki.

3. Przekazanie danych osobowych, których administratorem jest Administrator Danych do państwa trzeciego może nastąpić w sytuacji, jeżeli Komisja Europejska wydała decyzję, że dane państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony. Takie przekazanie nie wymaga specjalnego zezwolenia.

4. W przypadkach braku decyzji Komisji Europejskiej, o której mowa w pkt 3, dokonanie przekazania danych osobowych do państwa trzeciego jest możliwe, gdy Administrator Danych samodzielnie zapewni odpowiednie zabezpieczenia i pod warunkiem, że będą obowiązywały egzekwowalne prawa osób, których dane dotyczą i skuteczne środki ochrony prawnej. Odpowiednie zabezpieczenia Administrator Danych może zapewnić za pomocą:

   4.1. wiążących reguł korporacyjnych zatwierdzonych przez organ nadzorczy, mających zastosowanie do każdego z członków grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą,

   4.2. standardowych klauzul ochrony danych przyjętych lub zatwierdzonych przez Komisję Europejską,

   4.3. standardowych klauzul ochrony danych przyjętych przez organ nadzorczy i zatwierdzonych przez Komisję Europejską,

   4.4. zatwierdzonego kodeksu postępowania wraz z wiążącymi i egzekwowalnymi zobowiązaniami administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą, lub

   4.5. zatwierdzonego mechanizmu certyfikacji wraz z wiążącymi i egzekwowalnymi zobowiązaniami administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą.

5. Z zastrzeżeniem zezwolenia właściwego organu nadzorczego odpowiednie zabezpieczenia, o których mowa w pkt. 4 Administrator Danych może zapewnić w szczególności za pomocą:

   5.1. klauzul umownych między Administratorem Danych lub podmiotem przetwarzającym a Administratorem Danych, podmiotem przetwarzającym lub odbiorcą danych osobowych w państwie trzecim lub organizacji międzynarodowej, lub

6. w szczególnych przypadkach, dopuszcza się przekazanie danych osobowych przez Administratora Danych do państwa trzeciego pomimo braku decyzji Komisji Europejskiej, o której mowa w pkt 3 oraz zapewnienia odpowiednich zabezpieczeń, o których mowa w pkt 4 i 5. Do tych szczególnych przypadków zalicza się przekazanie danych pod warunkiem, że:

6.1. osoba, której dane dotyczą, poinformowana o ewentualnym ryzyku, z którymi może się dla niej wiązać proponowane przekazanie, wyrazi na nie wyraźną zgodę,

6.2. przekazanie jest niezbędne do wykonania umowy zawartej z osobą, której dane dotyczą,

6.3. przekazanie jest niezbędne do zawarcia lub wykonania umowy zawartej w interesie osoby, której dane dotyczą,

6.4. przekazanie jest niezbędne ze względu na ważne względy interesu publicznego,

6.5. przekazanie jest niezbędne ze względu na posiadane roszczenia,

6.6. przekazanie jest niezbędne do ochrony żywotnych interesów osoby, których dane dotyczą lub

6.7. przekazanie nastąpi z publicznego rejestru.

7. Osoba zarządzająca procesami przetwarzania danych osobowych przed planowanym przekazaniem danych do państwa trzeciego, jest zobowiązany poinformować o tym OBDO oraz skonsultować z nim warunki przekazania tych danych. Przekazanie danych może odbyć się wyłącznie na podstawie warunków i postanowień zaakceptowanych przez OBDO.

7. WSPÓŁADMINISTROWANIE DANYMI OSOBOWYMI

1. Administrator Danych w zakresie przetwarzanych przez siebie danych osobowych dopuszcza możliwość przyjęcia modelu współadministrowania danymi osobowymi zgodnie z art. 26 RODO.
2. Współadministrowanie danymi może zachodzić wówczas, jeżeli Administrator Danych oraz co najmniej jeden inny podmiot, wspólnie ustalają cele i sposoby przetwarzania danych osobowych. Oznacza to, że w danym procesie przetwarzania danych osobowych muszą zostać spełnione równocześnie trzy warunki, tj. Administrator Danych oraz co najmniej jeden inny podmiot muszą:
   2.1. być administratorami w rozumieniu art. 4 pkt 7 RODO,
   2.2. muszą wspólnie ustalić cele przetwarzania danych,
   2.3. muszą wspólnie ustalić sposoby (techniczne i organizacyjne) przetwarzania danych osobowych.
3. W przypadku spełnienia warunków, o których mowa w pkt 2 Administrator Danych oraz co najmniej jeden inny podmiot stają się współadministratorami danych w zakresie danego procesu przetwarzania danych osobowych.
4. W przypadku przyjęcia modelu współadministrowania danymi, współadministratorzy danych w drodze wspólnych uzgodnień, w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO.
5. W sytuacji, kiedy w zakresie zachodzących w strukturze Administratora Danych procesów przetwarzania danych osobowych pojawią się procesy, wobec których istnieje prawdopodobieństwo zachodzenia współadministrowania danymi, Osoba zarządzająca procesami przetwarzania danych osobowych informuje o tym fakcie OBDO.
6. OBDO dokonuje oceny, czy dany proces przetwarzania spełnia warunki współadministrowania danymi.
7. W przypadku, kiedy wynik oceny, o której mowa w pkt 6 wskazuje na współadministrowanie danymi osobowymi, OBDO, przy współudziale Osób zarządzających procesami przetwarzania danych osobowych oraz pozostałych współadministratorów, opracowuje wspólne uzgodnienia, o których mowa w pkt 4.

8. PODEJŚCIE OPARTE NA RYZYKU

1. W zakresie stosowanych rozwiązań odnoszących się do przetwarzania danych osobowych, a w szczególności w zakresie zabezpieczeń, Administrator Danych stosuje zasadę podejścia opartego na ryzyku (*risk-based approach*).

2. Administrator Danych uzależnia sposób realizacji nałożonych na niego obowiązków od charakteru, zakresu, kontekstu i celów przetwarzania danych oraz od ryzyka naruszenia praw i wolności osób, których dane dotyczą, a także ryzyka naruszenia interesów Administratora Danych.

3. Realizując zasadę podejścia opartego na ryzyku, Administrator Danych:

   3.1. respektuje to, że RODO szczególny nacisk kładzie na ochronę praw i wolności osób, których dane osobowe są przetwarzane,

   3.2. dostosowuje środki ochrony danych osobowych do skali ryzyka naruszenia praw i wolności osób fizycznych, których dane dotyczą,

   3.3. koncentruje się na poszukiwaniu i wdrażaniu środków redukujących prawdopodobieństwo i skutki wystąpienia najbardziej dotkliwych zagrożeń,

   3.4. dokonuje monitorowania i regularnych przeglądów procesów i sposobów organizacji przetwarzania danych osobowych.

4. Stosowana przez Administratora Danych zasada podejścia opartego na ryzyku jest procesem ciągłym, wymagającym stałej identyfikacji i szacowania poziomu ryzyka związanego z przetwarzaniem danych osobowych. W strukturze Administratora Danych następuje to, w szczególności poprzez:

   4.1. przeprowadzanie oceny ryzyka dla procesów lub sposobów organizacji przetwarzania danych osobowych (Podrozdział 9 Polityki),

   4.2. dokonywanie kwalifikacji procesów przetwarzania danych osobowych pod kątem stopnia występującego ryzyka naruszenia praw i wolności praw osób, których dane dotyczą (Podrozdział 11 Polityki),

   4.3. dokonywanie kwalifikacji procesów przetwarzania danych osobowych pod kątem konieczności poddania ich ocenie skutków dla ochrony danych osobowych (Podrozdział 11 Polityki),

   4.4. przeprowadzanie oceny skutków dla ochrony danych osobowych (Podrozdział 11 Polityki),

   4.5. stosowanie tzw. zasad *privacy by design* i *privacy by default* (Podrozdział 10 Polityki),

   4.6. przeprowadzanie audytów zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz procedurami wdrożonymi w strukturze Administratora Danych (Podrozdział 14 Polityki),

   4.7. przeprowadzanie testów równowagi prawnie uzasadnionego interesu Administratora Danych (Podrozdział 12 Polityki),

   4.8. stały monitoring otoczenia prawnego mającego wpływ na przetwarzanie danych osobowych przez Administratora Danych (monitoring zewnętrzny),

4.9. stały monitoring realizacji wypracowanych założeń w zakresie ochrony danych osobowych w ramach struktury Administratora Danych (monitoring wewnętrzny).

5. Skuteczność wdrożonych środków ochrony danych osobowych jest stale monitorowana i udoskonalana, w szczególności w ramach mechanizmu, o którym mowa w pkt. 4.6. tj. audytów zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz procedurami wdrożonymi w strukturze Administratora Danych.

9. OCENA RYZYKA DLA PROCESÓW LUB SPOSOBÓW ORGANIZACJI PRZETWARZANIA DANYCH OSOBOWYCH

1. Ocena ryzyka dla procesów lub sposobów organizacji przetwarzania danych osobowych przeprowadzana jest w sytuacjach, gdy istnieje uzasadnione podejrzenie, że dany proces lub sposób organizacji przetwarzania danych osobowych może nieść za sobą ryzyko naruszenia praw lub wolności osób, których dane dotyczą. W szczególności dotyczy to procesów lub sposobu organizacji przetwarzania danych osobowych, które wiążą się z zastosowaniem technologii, zarówno nowych jak i tych, które uległy znacznej zmianie w stosunku do ich pierwotnego charakteru lub zastosowania.
2. Procedura oceny ryzyka dla procesów lub sposobów organizacji przetwarzania danych osobowych stanowi Załącznik nr 6A do Polityki.

10. OCHRONA DANYCH OSOBOWYCH W FAZIE PROJEKTOWANIA ORAZ DOMYŚLNA OCHRONA DANYCH OSOBOWYCH

1. Administrator Danych wdraża odpowiednie środki techniczne i organizacyjne, zaprojektowane w celu skutecznej realizacji zasad ochrony danych osobowych, nadania przetwarzaniu danych niezbędnych zabezpieczeń oraz zapewnieniu ochrony praw osób, których dane dotyczą.
2. Wdrażając odpowiednie środki techniczne i organizacyjne Administrator Danych uwzględnia:
   2.1. stan wiedzy technicznej,
   2.2. koszt wdrażania,
   2.3. charakter, zakres, kontekst i cele przetwarzania danych,
   2.4. ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania.
3. Administrator Danych wdraża takie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia określonego celu przetwarzania, biorąc pod uwagę: ilość zbieranych danych osobowych, ich zakres, okres ich przechowywania oraz ich dostępność dla innych osób.
4. W szczególności, stosowane środki techniczne i organizacyjne muszą zapewnić, by domyślnie dane osobowe nie były udostępniane nieokreślonej liczbie osób.
5. W pierwszej kolejności, Administrator Danych rozważa, czy cel jakiemu ma służyć projektowane rozwiązane jest możliwy do osiągnięcia bez konieczności przetwarzania danych osobowych. Jeśli tak, należy wybrać takie rozwiązanie.
6. Administrator Danych zapewnia, aby spełnienie warunków wskazanych w pkt 1-5 (tzw. zasady *privacy by design* i *privacy by default*) było odpowiednio udokumentowane np. w formie notatki, maila, raportu z przeprowadzonych testów systemu informatycznego, wydruku z ekranu systemu.
7. Ogólny opis organizacyjnych środków bezpieczeństwa wdrożonych w strukturze Administratora Danych stanowi Załącznik nr 12 do Polityki.
8. Ogólny opis technicznych środków bezpieczeństwa wdrożonych w strukturze Administratora Danych stanowi Załącznik nr 13 do Polityki.

11. OCENA SKUTKÓW DLA OCHRONY DANYCH OSOBOWYCH (*DATA PROTECTION IMPACT ASSESSMENT*)

1. Administrator Danych dokonuje oceny skutków dla ochrony danych osobowych w celu opisania przetwarzania danych osobowych oraz oceny jego konieczności i proporcjonalności, a także w celu wspomagania zarządzania ryzykiem naruszenia praw i wolności osób fizycznych wynikającym z przetwarzania ich danych osobowych.
2. W strukturze Administratora Danych ocena skutków dla ochrony danych osobowych stanowi narzędzie rozliczalności ułatwiające przestrzeganie wymogów określonych w RODO, a także wykazanie, że podjęto odpowiednie środki w celu zapewnienia przestrzegania przepisów RODO.
3. Procedura oceny skutków dla ochrony danych osobowych (*data protection impact assessment*) stanowi Załącznik nr 7A do Polityki.

12. TEST RÓWNOWAGI PRAWNIE UZASADNIONEGO INTERESU ADMINISTRATORA DANYCH (*BALANCING TEST*)

1. W przypadkach, kiedy Administrator Danych przetwarza lub planuje przetwarzać dane osobowe na podstawie art. 6 ust. 1 lit. f) RODO tj. do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora Danych lub przez stronę trzecią, jest on zobowiązany do przeprowadzenia tzw. testu równowagi (*balancing test*).
2. Prawnie uzasadnione interesy Administratora Danych lub strony trzeciej, mogą być podstawą przetwarzania danych wyłącznie wtedy, o ile w świetle rozsądnych oczekiwań osób, których dane dotyczą, opartych na ich powiązaniach z Administratorem Danych nadrzędne nie są interesy lub podstawowe prawa i wolności osoby, której dane dotyczą.
3. Procedura testu równowagi prawnie uzasadnionego interesu Administratora Danych stanowi Załącznik nr 8 do Polityki.

13. INCYDENTY OCHRONY DANYCH OSOBOWYCH

1. Osobami odpowiedzialnymi za bezpieczeństwo danych osobowych, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do pomieszczeń oraz systemów, w których przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia incydentów ochrony danych osobowych, jest: Administrator Danych, OBDO oraz ASI (w odniesieniu do danych przetwarzanych w systemach informatycznych).
2. Procedura postępowania z incydentami ochrony danych osobowych stanowi Załącznik nr 5A do Polityki.

14. AUDYTY ZGODNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

1. Audyty zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz procedurami wdrożonymi w strukturze Administratora Danych przeprowadzane są przez OBDO.
2. OBDO przeprowadza audyt według opracowanego planu audytów.
2. OBDO przygotowuje plan audytów na okres nie krótszy niż kwartał i nie dłuższy niż rok z zaznaczeniem, że plan musi obejmować co najmniej jeden audyt.
3. Plan audytów OBDO przygotowuje w formie pisemnej, w tym elektronicznej i przedstawia Administratorowi Danych nie później niż na dwa tygodnie przed dniem rozpoczęcia okresu objętego planem.
4. W planie audytów OBDO uwzględnia, w szczególności:
    4.1. przedmiot, zakres oraz termin przeprowadzenia poszczególnych audytów oraz sposób i zakres ich dokumentowania,
    4.2. procesy przetwarzania danych osobowych objęte audytem,
    4.3. konieczność weryfikacji zgodności przetwarzania danych osobowych z:
        4.3.1. zasadami przetwarzania danych osobowych,
        4.3.2. zasadami dotyczącymi zabezpieczenia danych osobowych,
        4.3.3. zasadami przekazywania danych osobowych innym podmiotom.
5. W toku audytu OBDO dokonuje i dokumentuje czynności, w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz do opracowania sprawozdania.
6. Po zakończeniu audytu, OBDO przygotowuje dla Administratora Danych, sprawozdanie w tym zakresie. Sprawozdanie sporządzane jest w formie pisemnej, w tym elektronicznej.
7. OBDO przekazuje Administratorowi Danych sprawozdanie nie później niż w terminie 30 dni od zakończenia audytu.
8. Wzór sprawozdania z audytu stanowi Załącznik nr 10 do Polityki.

15. REALIZACJA PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ

1. Administrator Danych uwzględnia w zachodzących w jego strukturze procesach przetwarzania danych osobowych, procedury i zasady ułatwiające osobie, której dane dotyczą, wykonywanie praw przysługujących jej na mocy przepisów RODO, w tym, w szczególności:
   1.1. prawo do wycofania wyrażonej zgody (art. 7 ust. 3 RODO),
   1.2. prawo dostępu przysługujące osobie, której dane dotyczą (art. 15 RODO),
   1.3. prawo do sprostowania danych (art. 16 RODO),
   1.4. prawo do usunięcia danych (w tym prawo do bycia zapomnianym) (art. 17 RODO),
   1.5. prawo do ograniczenia przetwarzania (art. 18 RODO),
   1.6. prawo do przenoszenia danych (art. 20 RODO),
   1.7. prawo sprzeciwu (art. 21 RODO),
   1.8. prawo do niepodlegania decyzjom opartym wyłącznie na zautomatyzowanym przetwarzaniu (art. 22 RODO).
2. Procedura realizacji praw osób, których dane dotyczą stanowi Załącznik nr 9 do Polityki.

16. OGÓLNE ZASADY BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH

1. Dostęp do danych osobowych mogą mieć tylko pracownicy posiadający upoważnienie do ich przetwarzania.
2. Przebywanie osób nieuprawnionych do przetwarzania danych w pomieszczeniu, w którym przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do ich przetwarzania, chyba, że dane te są w odpowiedni sposób zabezpieczone przed dostępem.
3. Pracownicy mający dostęp do danych osobowych nie mogą ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem, w zakresie obowiązków służbowych, w ramach udzielonego upoważnienia do przetwarzania danych.
4. Pracownicy przechowujący dane osobowe zobowiązani są do zabezpieczenia materiałów zawierających dane osobowe w sposób uniemożliwiający dostęp do nich osobom nieuprawnionym.
5. Niedopuszczalnym jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia oraz jej bezpośredni przełożony.
6. Nikomu nie należy udostępniać indywidualnych haseł i identyfikatorów do systemów informatycznych.
7. Wysyłanie seryjnych wiadomości e-mail wymaga zastosowania opcji *kopia ukryta*.
8. Nie można udzielać informacji dotyczących danych osobowych innym podmiotom na podstawie prośby o takie dane skierowanej w formie zapytania telefonicznego.
9. W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej pracownicy zobowiązani są do stosowania zasady tzw. *czystego biurka*, która oznacza niepozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym. Za realizację zasady odpowiedzialny jest na swym stanowisku każdy z pracowników. Nie należy pozostawiać danych osobowych w miejscach ogólnodostępnych takich jak np. biurka, blaty, parapety.
10. Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe odbywać się musi w sposób uniemożliwiający odczytanie zawartej w nich treści, np. z wykorzystaniem niszczarek.
11. Za bezpieczeństwo przetwarzania danych osobowych w określonym procesie indywidualną odpowiedzialność ponosi przede wszystkim każdy pracownik mający dostęp do danych.
12. W czasie chwilowej nieobecności pracowników w pomieszczeniach, w godzinach pracy jak i po zakończeniu pracy, są oni zobowiązani do zamykania na klucz pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe.
13. Klucze do pomieszczeń, w których przetwarzane są dane osobowe nie mogą być pozostawione w zamku w drzwiach. Pracownicy zobowiązani są do dołożenia należytej staranności w celu zabezpieczenia kluczy przed udostępnieniem ich osobom nieupoważnionym.
14. Przed wyjściem z pomieszczenia, w którym przechowywane są dane osobowe należy upewnić się, że zostało ono odpowiednio zabezpieczone (zamknięte okna, drzwi).

15. Po zakończeniu pracy w systemie informatycznym, w którym przechowywane są dane osobowe, należy wylogować się z systemu.

16. Osoba użytkująca komputer przenośny zawierający dane osobowe zobowiązana jest do zachowania szczególnej ostrożności podczas jego transportu, przechowywania i użytkowania poza obszarem, w którym przetwarzane są dane osobowe.

17. Na pracowniku pracującym zdalnie spoczywa obowiązek odpowiedniego zabezpieczenia danych tak, aby osoby trzecie nie miały dostępu do danych osobowych.

17. PRZEGLĄDY I AKTUALIZACJA POLITYKI OCHRONY DANYCH OSOBOWYCH

1. Polityka podlega okresowemu przeglądowi pod kątem jej adekwatności, nie rzadziej niż raz do roku.
2. Przeglądu Polityki dokonuje OBDO. Dokonanie przeglądu Polityki może nastąpić, w szczególności w ramach przeprowadzanego przez OBDO audytu zgodności przetwarzania danych osobowych.
3. Przegląd powinien obejmować, w szczególności ocenę adekwatności Polityki do:
   3.1. procesów funkcjonujących w strukturach Administratora Danych,
   3.2. obowiązujących przepisów prawa odnoszących się do ochrony danych osobowych, którym podlega Administrator Danych.
4. W każdym przypadku, gdy zmianie ulegają przepisy prawa będące źródłem wskazanych w Polityce obowiązków lub zaistnieją istotne zmiany faktyczne w ramach struktury Administratora Danych przegląd Polityki wykonywany jest niezwłocznie.
5. Jeżeli w wyniku przeglądu Polityki stwierdzona zostanie konieczność aktualizacji jej zapisów, OBDO dokonuje aktualizacji Polityki w wymaganym zakresie.

18. ZAŁĄCZNIKI

Załącznik nr 1	Wykaz zbiorów danych osobowych wraz z procesami przetwarzania danych osobowych oraz Osobami zarządzającymi procesami przetwarzania danych osobowych
Załącznik nr 2	Zasady retencji danych osobowych
Załącznik nr 3	Procedura szkoleń oraz nadawania upoważnień do przetwarzania danych osobowych
Załącznik nr 4	Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych
Załącznik nr 5A	Procedura postępowania z incydentami ochrony danych osobowych
Załącznik nr 5B	Kalkulacja oceny ryzyka naruszenia
Załącznik nr 6A	Procedura oceny ryzyka dla procesów lub sposobów organizacji przetwarzania danych
Załącznik nr 6B	Matryca oceny ryzyka dla procesów lub sposobów organizacji przetwarzania danych
Załącznik nr 7A	Procedura oceny skutków dla ochrony danych osobowych (*data protection impact assessment*)
Załącznik nr 7B	Analiza preDPIA i ogólna ocena poziomu ryzyka dla procesu
Załącznik nr 8	Test równowagi prawnie uzasadnionego interesu Administratora Danych (*balancing test*)
Załącznik nr 9	Procedura realizacji praw osób, których dane dotyczą
Załącznik nr 10	Wzór sprawozdania z audytu zgodności przetwarzania danych osobowych
Załącznik nr 11	Procedura kontroli podmiotów przetwarzających
Załącznik nr 12	Ogólny opis organizacyjnych środków bezpieczeństwa
Załącznik nr 13	Ogólny opis technicznych środków bezpieczeństwa
Załącznik nr 14	Wzory wyznaczenia oraz odwołania Oficer Bezpieczeństwa Danych Osobowych
Załącznik nr 15	Wzory wyznaczenia oraz odwołania Administratora Systemów Informatycznych

Dokument sporządzono:	**Administrator Danych**
Data: 01/12/2021 Miejsce: Warszawa	…… *podpis, pieczęć*

Załącznik nr 1 – Wykaz zbiorów danych osobowych wraz z procesami przetwarzania danych osobowych oraz osobami zarządzającymi procesami przetwarzania danych osobowych

Lp.	Zbiór danych osobowych	Proces przetwarzania danych osobowych	Osoba zarządzająca procesami przetwarzania danych osobowych *(imię, nazwisko, stanowisko, dane kontaktowe)*
1.	**CZŁONKOWIE**	Rekrutacja	Paulina Kołodziejczyk, Sekretarz Generalny IFMSA-Poland sekretarz@ifmsa.pl
		Realizacja zadań statutowych	Patryk Groszyk, Wiceprezydent IFMSA-Poland ds. wewnętrznych vpi@ifmsa.pl
		Oddziały lokalne	Patryk Groszyk, Wiceprezydent IFMSA-Poland ds. wewnętrznych vpi@ifmsa.pl
		Osoby funkcyjne w IFMSA-Poland	Paulina Kołodziejczyk, Sekretarz Generalny IFMSA-Poland sekretarz@ifmsa.pl
		Lista mailingowa	Paulina Kołodziejczyk, Sekretarz Generalny IFMSA-Poland sekretarz@ifmsa.pl

2.	**ALUMNI**	Przystąpienie do programu absolwentów	Mariola Piekarska, Prezydent IFMSA-Poland prezydent@ifmsa.pl
3.	**WYMIANY**	Program stały SCOPE	Maciej Mach, Koordynator Narodowy ds. praktyk klinicznych NEO-out neo-out@ifmsa.pl
		Program stały SCORE	Maciej Lazarek, Koordynator Narodowy ds. wymiany naukowej nore@ifmsa.pl
		Inne programy	Maciej Mach, Koordynator Narodowy ds. praktyk klinicznych NEO-out neo-out@ifmsa.pl
4.	**WSPÓŁPRACE**	Zawieranie i realizacja umów	Maja Woźniakowska, Wiceprezydent IFMSA-Poland ds. marketingu vpe@ifmsa.pl
		Dochodzenie roszczeń, obrona przed roszczeniami	Maja Woźniakowska, Wiceprezydent IFMSA-Poland ds. marketingu vpe@ifmsa.pl
5.	**MARKETING**	Konkursy	Wiktoria Mika, Wiceprezydent IFMSA-Poland ds.

			wizerunku i komunikacji media@ifmsa.pl
		Eventy	Wiktoria Mika, Wiceprezydent IFMSA-Poland ds. wizerunku i komunikacji media@ifmsa.pl
		Formularz kontaktowy	Wiktoria Mika, Wiceprezydent IFMSA-Poland ds. wizerunku i komunikacji media@ifmsa.pl
6.	**KONTRAHENCI**	Zawieranie i realizacja umów	Mariola Piekarska, Prezydent IFMSA-Poland prezydent@ifmsa.pl
		Dochodzenie roszczeń, obrona przed roszczeniami	Mariola Piekarska, Prezydent IFMSA-Poland prezydent@ifmsa.pl
7.	**KORESPONDENCJA**	Ewidencjonowanie korespondencji IFMSA-Poland	Paulina Kołodziejczyk, Sekretarz Generalny IFMSA-Poland sekretarz@ifmsa.pl

Załącznik nr 2 – Zasady retencji danych osobowych

RODO nakłada na Administratora Danych obowiązek przechowywania danych w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

Po osiągnięciu celu dane osobowe powinny zostać usunięte lub poddane anonimizacji. W tym celu, Administrator Danych jest zobowiązany do stałego nadzorowania zawartości administrowanych zbiorów danych oraz występujących w ich ramach procesów przetwarzania, pod kątem konieczności usuwania danych zbędnych, albo do których przetwarzania przestał być upoważniony.

Zasady ustalania okresu retencji danych osobowych

1. Ustalając okres retencji danych osobowych należy od początku procesu przetwarzania ustalić jego cel i stale monitorować czy z upływem czasu cel ten jest nadal aktualny.
2. Ustalając okres retencji należy wziąć pod uwagę, czy przepisy szczególne nie określają przez jaki czas należy przechowywać dane (np. prawo pracy). W sytuacji, gdy do jednego procesu przetwarzania danych osobowych zastosowanie mają różne przepisy, należy wybrać przepis najbardziej adekwatny.
3. W sytuacji, gdy nie ma przepisów prawa ustalających okres retencji, Administrator Danych jest zobowiązany do samodzielnego ustalenia okresów retencji dla poszczególnych procesów na zasadzie adekwatności. Należy również mieć na uwadze fakt, że z upływem czasu przydatność danych maleje, a dane często stają się nieaktualne.
4. Należy ustalić, kiedy rozpoczyna się i kończy okres retencji:
    4.1. w sytuacji, gdy można określić dokładnie początek okresu retencji (np. otrzymanie danych) należy wyliczyć okres retencji zgodnie z wewnętrznymi regulacjami (np. 3 lata po zebraniu danych, 5 lat po wygaśnięciu umowy o pracę),
    4.2. w sytuacji, gdy nie jest możliwe dokładnie określenie początku okresu retencji, jej koniec powinno określać konkretne zdarzenie (np. CV kandydatów powinny być usunięte niezwłocznie po zakończeniu procesu rekrutacji).
5. W pewnych sytuacjach okres retencji może ulegać wydłużeniu lub skróceniu:
    5.1. okres retencji ulega wydłużeniu np. gdy dane są przetwarzane dla dwóch różnych celów (tj. wykonanie umowy i dla celów dowodowych),
    5.2. okres retencji ulega skróceniu np. gdy osoba, której dane dotyczą wniesie zasadny sprzeciw wobec przetwarzania jej danych osobowych albo właściwy organ publiczny zwróci się z żądaniem usunięcia określonych danych – w takiej sytuacji należy zdecydować jakie dane należy usunąć, a jakie zostawić, ze względu na nadrzędny cel np. przepis prawa.
6. Należy wprowadzić wewnętrzne regulacje, które określą okresy retencji dla wszystkich procesów przetwarzania danych osobowych. Przy określeniu okresu retencji należy wziąć pod uwagę, w szczególności:
    6.1. rodzaj danych osobowych,

6.2. cel przetwarzania,

6.3. właściwe przepisy prawa.

7. Należy ustalić osoby odpowiedzialne za retencje danych osobowych w poszczególnych procesach przetwarzania danych osobowych.

Zasady stosowania retencji danych osobowych

1. Rozpoczynając proces usuwania danych należy wziąć pod uwagę czas, który jest potrzebny na znalezienie i usunięcie tych danych (np. jeżeli uznaje się, że usuniecie danych zajmie tydzień, należy rozpocząć ten proces najpóźniej tydzień przed upływem okresu retencji).

2. Należy ustalić metody usuwania danych, uwzględniając podział na dane osobowe przechowywane w formie papierowej i elektronicznej oraz mając na uwadze przepisy prawa i inne regulacje wewnętrzne.

Anonimizacja jako alternatywa dla usuwania danych osobowych

1. W sytuacji, gdy kończy się okres retencji, a dane są nadal potrzebne (np. do celów statystycznych czy analitycznych) można zachować te dane pod warunkiem ich anonimizacji.

2. Anonimizacja oznacza przekształcenie danych osobowych w sposób uniemożliwiający przyporządkowanie poszczególnych informacji do określonej lub możliwej do zidentyfikowania osoby fizycznej albo jeżeli przyporządkowanie takie wymagałoby niewspółmiernych kosztów, czasu lub działań.

W związku z informacjami zawartymi w niniejszym Załączniku, dla danych osobowych przetwarzanych przez Administratora Danych jako ich administratora w rozumieniu art. 4 pkt 7 RODO, ustala się następujące terminy retencji.

Zbiór danych osobowych	Proces przetwarzania danych osobowych	Retencja danych
CZŁONKOWIE	Rekrutacja	do czasu wycofania zgody, nie dłużej jednak niż przez okres 7 lat
	Realizacja zadań statutowych	do czasu przedawnienia ewentualnych roszczeń
	Oddziały lokalne	do czasu przedawnienia ewentualnych roszczeń
	Osoby funkcyjne w IFMSA-Poland	przez czas trwania kadencji
	Lista mailingowa	do czasu wniesienia sprzeciwu
ALUMNI	Przystąpienie do programu absolwentów	do czasu wycofania zgody
WYMIANY	Program stały SCOPE	przez czas trwania programu, a po tym przez okres przedawnienia ewentualnych roszczeń
	Program stały SCORE	przez czas trwania programu, a po tym przez okres przedawnienia ewentualnych roszczeń
	Inne programy	przez czas trwania programu, a po tym przez okres przedawnienia ewentualnych roszczeń

WSPÓŁPRACE	Zawieranie i realizacja umów	przez okres wynikający z przepisów prawa - 6 lat od zakończenia współpracy
	Dochodzenie roszczeń, obrona przed roszczeniami	Przez okres 6 lat od wystąpienia roszczenia (lub do momentu rozstrzygnięcia sporu) z uwzględnieniem właściwych terminów przedawnienia roszczeń.
MARKETING	Konkursy	do czasu wycofania zgody, nie dłużej niż do czasu zakończenia konkursu. Po tym okresie przez czas przedawnienia ewentualnych roszczeń.
	Eventy	do czasu zakończenia eventu, a po tym okresie przez czas przedawnienia ewentualnych roszczeń
	Formularz kontaktowy	do czasu udzielenia odpowiedzi na wiadomość przesłaną przez formularz kontaktowy
KONTRAHENCI	Zawieranie i realizacja umów	przez okres wynikający z przepisów prawa - 6 lat od zakończenia współpracy
	Dochodzenie roszczeń, obrona przed roszczeniami	Przez okres 6 lat od wystąpienia roszczenia (lub do momentu rozstrzygnięcia sporu) z uwzględnieniem właściwych terminów przedawnienia roszczeń.
KORESPONDENCJA	Ewidencjonowanie korespondencji IFMSA-Poland	Okres przechowywania dokumentacji stanowiącej przedmiot uzależniony jest od tego, czego dana dokumentacja dotyczy. W tym zakresie stosuje się okresy retencji właściwe dla danego procesu.

Załącznik nr 3 – Procedura szkoleń oraz nadawania upoważnień do przetwarzania danych osobowych

1. Upoważnienia do przetwarzania danych osobowych nadawane są przez Administratora Danych. Administrator Danych może upoważnić konkretną osobę do udzielania w jego imieniu upoważnień do przetwarzania danych osobowych.
2. Osobą odpowiedzialną za administrowanie oraz kontrolę upoważnień do przetwarzania danych osobowych jest OBDO.
3. Osobami odpowiedzialnymi za informowanie OBDO o konieczności nadania upoważnienia do przetwarzania danych osobowych, jego zmiany lub odwołania, są Wiceprezydent IFMSA-Poland ds. zasobów ludzkich oraz Wiceprezydenci Oddziałów ds. zasobów ludzkich.
4. Szczegółowa procedura nadawania upoważnień do przetwarzania danych osobowych, ich zmiany lub odwołania, została wskazana poniżej.

Nadanie upoważnienia

1. W przypadku zatrudnienia nowego pracownika lub objęcia funkcji przez Członka, który w ramach swoich obowiązków służbowych będzie przetwarzał dane osobowe, istnieje konieczność nadania mu stosownego upoważnienia do przetwarzania danych osobowych. To samo tyczy się sytuacji, w której dochodzi do zmiany stanowiska pracownika, która łączy się z uzyskaniem dostępu do danych osobowych.
2. Przedstawiciel Administratora wysyła OBDO drogą elektroniczną na adres email obdo@ifmsa.pl wniosek o nadanie upoważnienia.
3. Wniosek o nadanie upoważnienia stanowi tabela w pliku Excel, która zawiera:
   3.1. imię i nazwisko upoważnianego,
   3.2. stanowisko upoważnianego,
   3.3. Oddział upoważnianego,
   3.4. zbiory danych, do których upoważniany będzie miał dostęp.
4. OBDO przed nadaniem pracownikowi upoważnienia, organizuje dla niego krótkie szkolenie, podczas którego informuje go o podstawowych aspektach prawnych związanych z ochroną danych osobowych (najważniejsze definicje, odpowiedzialność prawna, obowiązek właściwego zabezpieczenia danych przetwarzanych w formie papierowej oraz w systemach informatycznych).
5. Szkolenie jest przeprowadzone w formie tradycyjnej w siedzibie Administratora Danych lub miejscu przez niego wskazanym lub w formie elektronicznej.
6. W przypadku szkolenia w formie tradycyjnej:
   6.1. OBDO na podstawie otrzymanego wniosku sporządza listę osób uczestniczących w szkoleniu tradycyjnym,

6.2. OBDO przeprowadza szkolenie w siedzibie Administratora Danych lub miejscu wskazanym przez Administratora Danych,

6.3. Potwierdzeniem ukończenia szkolenia jest pozytywny wynik testu wiedzy przeprowadzonego przez OBDO w formie elektronicznej.

7. W przypadku szkolenia w formie online:

7.1. OBDO na podstawie otrzymanego wniosku sporządza listę osób uczestniczących w szkoleniu online,

7.2. Przedstawiciele Administratora udostępniają uczestnikom kursu materiały do nauki, w tym szkolenie w formie nagrania,

7.3. Potwierdzeniem ukończenia szkolenia jest pozytywny wynik testu wiedzy przeprowadzonego przez OBDO w formie elektronicznej.

8. Szkolenie zakończone jest testem wiedzy.

9. Osobie, która ukończyła szkolenie nadawane jest upoważnienie do przetwarzania danych osobowych.

10. Upoważnienie nadawane jest w formie pisemnej (w tym w postaci elektronicznej).

11. Upoważnienie w postaci elektronicznej nie wymaga odręcznego podpisu osoby upoważniającej oraz upoważnianego.

12. Upoważnienia w postaci elektronicznej przechowywane są w formacie .pdf.

13. Wydanie każdego upoważnienia jest odnotowywane przez OBDO w prowadzonej przez niego ewidencji osób upoważnionych do przetwarzania danych osobowych.

14. Każde wydane upoważnienie posiada unikalną sygnaturę o wzorze U/Nr upowiażnienia/Rok

15. Ewidencja osób upoważnionych do przetwarzania danych osobowych jest prowadzona przez OBDO w postaci elektronicznej.

Zmiana zakresu upoważnienia

1. Zakres nadanego pracownikowi upoważnienia może ulegać zmianie (rozszerzeniu bądź zawężeniu) w związku z pełnieniem przez niego określonych zadań w określonym przedziale czasu.

2. W przypadku zmiany stanowiska pracy łączącej się ze zmianą zakresu danych, które przetwarza pracownik, istnieje konieczność złożenia wniosku o zmianę upoważnienia.

3. W przypadku konieczności zmiany upoważnienia, Przedstawiciel Administratora wysyła OBDO drogą elektroniczną na adres email obdo@ifmsa.pl wniosek o zmianę nadanego upoważnienia.

4. Wniosek o zmianę upoważnienia stanowi tabela w pliku Excel, która zawiera:

4.1. imię i nazwisko upoważnianego,

4.2. nowe stanowisko upoważnianego,

4.3. zbiory danych, do których upoważniany będzie miał dostęp w związku ze zmianą stanowiska.

5. Na podstawie otrzymanego wniosku OBDO zmienia zakres upoważnienia.

6. Zmiana zakresu wydanego upoważnienia jest odnotowywana przez OBDO w prowadzonej ewidencji upoważnień.

Odwołanie upoważnienia

1. Utrata prawa do przetwarzania danych osobowych określonych w upoważnieniu następuje w szczególności w przypadku:

   1.1. zakończenia kadencji na stanowisku, najczęściej z dniem 30 września, chyba że Przedstawiciel Administratora wskaże inny okres ważności upoważnienia (data ważności upoważnienia widnieje na Upoważnieniu)

   1.2. zmiany stanowiska pracy na stanowisko, na którym nie ma konieczności posiadania dostępu do danych osobowych lub w szczególności, gdy ustaje zasadność i celowość dalszego wykonywania prawa do przetwarzania danych w związku ze zmianą realizowanych przez pracownika zadań wynikających z jego indywidualnego zakresu czynności,

   1.3. umyślnego naruszenia zasad ochrony danych osobowych określonych w Ustawie, RODO lub Polityce,

   1.4. rozwiązania stosunku pracy,

   1.5. rozwiązania umowy cywilnoprawnej.

2. W przypadku punktów 1.2. – 1.5. Przedstawiciel Administratora wysyła OBDO drogą elektroniczną na adres email obdo@ifmsa.pl wniosek o odwołanie upoważnienia.

3. Wniosek o odwołanie upoważnienia stanowi tabela w pliku Excel, która zawiera:

   3.1. imię i nazwisko osoby, której ma zostać odwołane upoważnienie,

   3.2. stanowisko osoby, której ma zostać odwołane upoważnienie,

   3.3. wskazanie przyczyny odwołania upoważnienia.

4. Na podstawie wniosku OBDO odwołuje upoważnienie.

5. W przypadku odwołania upoważnienia na podstawie punktów 1.2. – 1.5. Przedstawiciel Administratora informuję mailowo osobę, która traci upoważnienie.

6. Odwołanie upoważnienia następuje poprzez jego wycofanie w ewidencji upoważnień prowadzonej przez OBDO.

SYG. U/NR UPOWAŻNIENIA/ROK

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Niniejszym, w imieniu **Międzynarodowe Stowarzyszenie Studentów Medycyny – IFMSA-Poland** (Administrator Danych), na podstawie art. 29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Ogólne rozporządzenie o ochronie danych) (RODO), **upoważniam:**

Imię i nazwisko upoważnianej osoby	Zbiory danych objęte zakresem upoważnienia	Data nadania upoważnienia
[imię, nazwisko]	[zbiory danych]	[data nadania oraz ważności upoważnienia] Upoważnienie jest ważne do czasu zakończenia kadencji, stosunku pracy, stosunku cywilnoprawnego lub odwołania

.....

Data i podpis upoważniającego

Osoba upoważniona zobowiązana jest przetwarzać dane osobowe zawarte w ww. zbiorach danych osobowych w zakresie i w sposób wymagany do wypełnienia obowiązków służbowych względem Administratora Danych.

Osoba upoważniona zobowiązuje się do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem oraz z przepisami RODO, wydanymi na jego podstawie krajowymi aktami wykonawczymi, w szczególności obowiązującej Ustawy o ochronie danych osobowych (Ustawa) i obowiązującymi w strukturze Administratora Danych wewnętrznymi regulacjami w sprawie ochrony danych osobowych.

Naruszenie ww. obowiązków może skutkować poniesieniem odpowiedzialności karnej na podstawie przepisów określonych w Ustawie oraz stanowi ciężkie naruszenie obowiązków pracowniczych, które może być podstawą rozwiązania umowy o pracę w trybie art. 52 Kodeksu Pracy lub odpowiedzialności cywilnej.

Oświadczenie

Oświadczam, że zapoznałam/em się, w zakresie wynikającym z przydzielonych zadań, z obowiązującymi w odniesieniu do ochrony danych osobowych przepisami prawa i regulacjami wewnętrznymi obowiązującymi w strukturze Administratora Danych (w szczególności z wyciągiem Polityki ochrony danych osobowych). Przyjmuję do wiadomości zawarte w nich obowiązki dotyczące ochrony danych osobowych i zobowiązuję się do ich stosowania.

Świadoma/y jestem obowiązku ochrony danych osobowych na zajmowanym stanowisku i w zakresie udzielonego mi upoważnienia do przetwarzania danych osobowych, a w szczególności obowiązku

zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po ustaniu zatrudnienia lub współpracy.

Załącznik nr 4 – Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych

Lp.	Sygnatura upoważnienia	Nazwisko osoby upoważnionej	Imię osoby upoważnionej	Oddział	Funkcja w Stowarzyszeniu	Data nadania upoważnienia	Data ustania upoważnienia	Nazwy zbiorów objętych zakresem upoważnienia
1.								
2.								
3.								
4.								
5.								
6.								
7.								

Załącznik nr 5A – Procedura postępowania z incydentami ochrony danych osobowych

1. Podmiotami odpowiedzialnymi za bezpieczeństwo danych osobowych, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do pomieszczeń oraz systemów, w których przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń, są:

   1.1. Administrator Danych,

   1.2. OBDO,

   1.3. ASI (w odniesieniu do danych przetwarzanych w systemach informatycznych).

2. Za naruszenie ochrony danych osobowych uważa się 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.

3. Żeby zaistniało naruszenie ochrony danych osobowych, muszą zostać spełnione łącznie trzy przesłanki:

   3.1. naruszenie musi dotyczyć danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych przez Administratora Danych,

   3.2. skutkiem naruszenia może być zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych;

   3.3. naruszenie jest skutkiem złamania zasad bezpieczeństwa danych.

4. Wyróżnia się trzy typy naruszeń danych osobowych:

   4.1. naruszenie poufności – polega na ujawnieniu danych osobowych nieuprawnionej osobie (*np. przypadkowe wysłanie danych osobowych do osoby postronnej*),

   4.2. naruszenie dostępności – polega na czasowej bądź trwałej utracie lub zniszczeniu danych osobowych (*np. zgubienie lub kradzież nośnika zawierającego dane osobowe przy braku kopii zapasowej*),

   4.3. naruszenie integralności – polega na zmianie treści danych osobowych w sposób nieautoryzowany (*np. pracownik dla żartu zmienia nazwiska klientów poprzez dopisanie litery „s" na końcu każdego z nich*).

5. Naruszenia mogą dotyczyć zarówno danych osobowych przetwarzanych w formie elektronicznej, jak i papierowej.

6. Pracownik, który powziął wiadomość o złamaniu lub podejrzeniu złamania zasad przetwarzania danych, a w szczególności o sytuacjach udostępnienia danych osobom nieuprawnionym, jest zobowiązany do niezwłocznego (lecz nie później niż w ciągu godziny od zdarzenia) powiadomienia:

   6.1. OBDO,

6.2. oraz ASI (w przypadku, jeżeli sytuacja dotyczy systemu informatycznego).

7. Powiadomienie, o którym mowa w pkt 6 powinno zawierać co najmniej następujące informacje:

7.1. data i miejsce naruszenia,

7.2. kategorie danych oraz przybliżoną liczbę osób, których dotyczy naruszenie,

7.3. opis naruszenia,

7.4. możliwe konsekwencje naruszenia,

7.5. informacje o ewentualnym podjęciu środków zaradczych.

8. Do czasu powiadomienia OBDO lub ASI, pracownik:

8.1. zabezpiecza dostęp do miejsca lub urządzenia,

8.2. wstrzymuje pracę na komputerze, na którym zaistniało naruszenie ochrony oraz nie uruchamia bez koniecznej potrzeby komputerów i innych urządzeń, które w związku z naruszeniem ochrony zostały wstrzymane,

8.3. podejmuje, stosownie do zaistniałej sytuacji inne, niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.

9. Dokonywanie zmian w miejscu naruszenia ochrony danych bez uzyskania zgody OBDO lub ASI jest możliwe tylko w sytuacji, jeżeli zachodzi konieczność ratowania osób lub mienia albo zapobieżenia grożącemu niebezpieczeństwu.

10. Zasady informowania Administratora Danych przez podmiot przetwarzający o naruszeniu ochrony powierzonych mu do przetwarzania danych osobowych, określa zawarta z tym podmiotem umowa powierzenia przetwarzania danych osobowych.

11. OBDO lub ASI, który wykrył lub został poinformowany o nieprawidłowościach przy przetwarzaniu danych osobowych powinien niezwłocznie zidentyfikować problem, zabezpieczyć dane i przedsięwziąć wszelkie niezbędne kroki, aby uniknąć w przyszłości podobnych zdarzeń.

12. OBDO lub ASI, po otrzymaniu zgłoszenia o naruszeniu dokonuje czynności sprawdzających, w tym w szczególności:

12.1. ocenia zaistniałą sytuację, biorąc pod uwagę w szczególności stan pomieszczeń, w których przetwarzane są dane osobowe, stan urządzeń i zbioru danych,

12.2. zabezpiecza oraz utrwala wszelkie informacje i dokumenty mogące stanowić pomoc przy ustaleniu przyczyn naruszenia, jak również sprawdza zawartość zbioru danych osobowych, w ramach którego doszło do naruszenia,

12.3. odbiera wyjaśnienia od osób, które uczestniczyły w naruszeniu oraz innych osób, które merytorycznie odpowiadają za procesy przetwarzania danych, w ramach których doszło do naruszenia,

12.4. sprawdza stan urządzeń wykorzystywanych do przetwarzania danych osobowych,

12.5. sprawdza sposób działania systemu (w tym również obecność wirusów komputerowych),

12.6. ustala charakter i rodzaj naruszenia oraz metody działania osób naruszających zabezpieczenie systemu,

12.7. dokonuje analizy stanu systemu wraz z oszacowaniem rozmiaru szkód powstałych w skutek naruszenia oraz poddaje analizie metody pracy osób upoważnionych do przetwarzania danych osobowych,

12.8. podejmuje decyzję o toku dalszego postępowania, stosownie do zakresu naruszenia lub zasadności podejrzenia naruszenia ochrony danych osobowych i w uzasadnionych przypadkach niezwłocznie powiadamia właściwą osobę podejmującą decyzję w imieniu Administratora Danych.

13. Na podstawie informacji uzyskanych w toku czynności sprawdzających, OBDO dokonuje kwalifikacji naruszenia. Naruszenie kwalifikowane jest jako:

13.1. nieskutkujące ryzykiem naruszenia praw lub wolności osób fizycznych,

13.2. skutkujące ryzykiem naruszenia praw lub wolności osób fizycznych,

13.3. skutkujące wysokim ryzykiem naruszenia praw lub wolności osób fizycznych.

14. Dokonując oceny ryzyka naruszenia praw lub wolności osób fizycznych OBDO bierze pod uwagę następujące kryteria:

14.1. charakter i wrażliwość danych osobowych, których dotyczy naruszenie,

14.2. rodzaj danych osobowych, których dotyczy naruszenie,

14.3. konsekwencje, jakie naruszenie wywołuje względem osoby, których dane dotyczą,

14.4. łatwość identyfikacji osoby, której dane dotyczą,

14.5. charakter podmiotu, któremu zostały ujawnione dane osobowe,

14.6. cechy szczególne osoby, której dane dotyczą, w tym w szczególności czy należy ona do grupy wymagającej szczególnej opieki,

14.7. publiczną dostępność do danych osobowych, których dotyczy naruszenie,

14.8. aktualność i poprawność merytoryczną danych, których dotyczy naruszenie,

które to kryteria zostały wskazane w wytycznych przyjętych przez Europejską Radę Ochrony Danych (Wytyczne dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679, przyjęte w dniu 3 października 2017 r., ostatnio zmienione i przyjęte w dniu 6 lutego 2018 r., WP250rev.01).

15. Na podstawie wskazanych wyżej w pkt 15 kryteriów, dokonuje się automatycznej kalkulacji ryzyka. Kalkulacja pozwala ustalić, czy naruszenie niesie za sobą ryzyko naruszenia praw lub wolności osób fizycznych i czy to ryzyko jest wysokie. Automatycznej kalkulacji dokonuje się z wykorzystaniem formularza stanowiącego Załącznik nr 5B do Polityki.

16. Każdy przypadek naruszenia, bądź podejrzenia naruszenia ochrony danych osobowych, powinien być poddany dodatkowej, obok automatycznej kalkulacji, analizie. Z tego względu automatyczna kalkulacja ryzyka stanowi jedynie dodatkowe źródło pomocnicze i nie może być samodzielną podstawą podejmowania decyzji.

17. W związku z zastrzeżeniem wskazanym w pkt 16, na ostateczny wynik kwalifikacji naruszenia mają wpływ dodatkowe czynniki indywidualne, uwzględnione przez OBDO w toku czynności sprawdzających, w szczególności zaliczymy do nich:

    17.1. rodzaj naruszenia,

    17.2. ilość danych osobowych,

    17.3. cechy szczególne administratora danych,

    17.4. liczbę osób fizycznych, na które naruszenie wywiera wpływ,

    17.5. okoliczności w jakich doszło do naruszenia,

    17.6. stosowane przez Administratora Danych zabezpieczenia danych osobowych, których dotyczy naruszenie.

18. Dokonując kwalifikacji naruszenia, o której mowa w pkt 14 konieczne jest również uwzględnienie:

    18.1. powagi zdarzenia, tj. wielkości szkody, jakie zdarzenie to może spowodować w odniesieniu do osoby, której dane dotyczą oraz

    18.2. prawdopodobieństwa wystąpienia tego zdarzenia będącego skutkiem naruszenia.

19. Oceniając ryzyko naruszenia praw i wolności osób, których dane dotyczą, OBDO powinien przyjąć perspektywę osób, których dane są przetwarzane i właśnie z tej perspektywy oceniać stopień dotkliwości w przypadku zmaterializowania się zagrożenia.

20. Nie jest konieczne, aby ryzyko naruszenia praw i wolności osób, których dane dotyczą się zmaterializowało (by faktycznie doszło do naruszenia praw lub wolności). OBDO, który ocenił wielkość potencjalnej szkody, które naruszenie może spowodować, biorąc pod uwagę kontekst i okoliczności całego zdarzenia, powinien ocenić prawdopodobieństwo jego zaistnienia.

21. OBDO, niezwłocznie po dokonaniu czynności sprawdzających sporządza, Protokół z naruszenia ochrony danych osobowych według wzoru, który znajduje się w niniejszym Załączniku.

22. Jeżeli naruszenie zostanie zakwalifikowane jako skutkujące ryzykiem naruszenia praw lub wolności osób fizycznych, OBDO przygotowuje zgłoszenie naruszenia do organu nadzorczego poprzez wypełnienie odpowiedniego formularza dostępnego na stronie internetowej organu nadzorczego. W zgłoszeniu podaje się następujące informacji:

    22.1. opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazanie kategorii i przybliżonej liczby osób, których dane dotyczą, oraz kategorii i przybliżonej liczby wpisów danych osobowych, których dotyczy naruszenie,

22.2. wskazanie imienia i nazwiska oraz danych kontaktowych IOD/OBDO lub oznaczenia innego punktu kontaktowego, od którego można uzyskać więcej informacji,

22.3. opis możliwych konsekwencji naruszenia ochrony danych osobowych,

22.4. wskazanie środków, jakie zostały zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

23. Przygotowane przez OBDO zgłoszenie naruszenia, Administrator Danych przekazuje do organu nadzorczego niezwłocznie, lecz nie później niż w ciągu 72 godzin po otrzymaniu Protokołu z naruszenia ochrony danych osobowych, w którym stwierdzone zostało naruszenie. Do zgłoszenia przekazanego po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

24. Zgłoszenia można dokonać za pomocą formularza dostępnego na stronie uodo.gov.pl na 4 sposoby:

24.1. elektronicznie poprzez wypełnienie dedykowanego formularza dostępnego bezpośrednio na platformie biznes.gov.pl,

24.2. elektronicznie poprzez wysłanie wypełnionego formularza na elektroniczną skrzynkę podawczą ePUAP: UODO/SkrytkaESP,

24.3. elektronicznie poprzez wysłanie wypełnionego formularza za pomocą pisma ogólnego dostępnego na platformie biznes.gov.pl,

24.4. tradycyjną pocztą, wysyłając wypełniony formularz na adres Urzędu.

25. Administrator Danych lub OBDO (na podstawie upoważnienia Administratora Danych) w celu wyjaśnienia sprawy, w zależności od potrzeby, prowadzi korespondencję z organem nadzorczym udzielając wszelkich niezbędnych informacji.

26. Jeżeli naruszenie zostanie zakwalifikowane jako skutkujące wysokim ryzykiem naruszenia praw lub wolności osób fizycznych, Administrator Danych informuje osobę, której dane dotyczą, o takim naruszeniu. W szczególności, w skierowanym zawiadomieniu, Administrator Danych podaje osobie, której dane zostały naruszone następujące informacje:

26.1. charakter naruszenia ochrony danych osobowych,

26.2. imię i nazwisko oraz dane kontaktowe OBDO lub innego punktu kontaktowego, od którego można uzyskać więcej informacji,

26.3. opis możliwych konsekwencji naruszenia ochrony danych osobowych,

26.4. opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu - w tym w stosownych przypadkach - środków w celu zminimalizowania jego ewentualnych negatywnych skutków.

27. OBDO przygotowuje treść zawiadomienia, o którym mowa w pkt 28 oraz rekomenduje formę, w jakiej ma nastąpić zawiadomienie. Komunikat kierowany do osoby, której dane dotyczą musi być jasny i zrozumiały oraz zawierać spójne i logiczne zalecenia dostosowane do konkretnej sytuacji.

28. Zawiadomienie, o którym mowa w pkt 28 nie jest wymagane w następujących przypadkach:

    28.1. Administrator Danych wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych,

    28.2. Administrator Danych zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,

    28.3. wymagałoby ono niewspółmiernie dużego wysiłku - w takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

29. Jeżeli naruszenie danych osobowych ma znamiona przestępstwa, wówczas Administrator Danych lub OBDO (na podstawie upoważnienia Administratora Danych) informuje odpowiednie organy ścigania.

30. W stosunku do osoby, która zaniedbuje obowiązki związane z ochroną danych osobowych mogą zostać wyciągnięte konsekwencje dyscyplinarne przewidziane Kodeksem Pracy oraz wewnętrznymi regulacjami obowiązującymi w strukturze Administratora Danych.

31. OBDO prowadzi rejestr naruszeń ochrony danych osobowych, według wzoru, który znajduje się w niniejszym Załączniku.

PROTOKÓŁ Z NARUSZENIA OCHRONY DANYCH OSOBOWYCH NR .../……

……

miejscowość, data

1. Administrator Danych: …

2. Oficer Bezpieczeństwa Danych Osobowych(*imię, nazwisko*): …

3. Osoba zgłaszająca naruszenie (*imię, nazwisko, stanowisko*): …

4. Osoby prowadzące czynności sprawdzające (*imiona, nazwiska, stanowiska*): …

5. Osoby udzielające informacji na temat naruszenia (*imiona, nazwiska, stanowiska*): …

6. Inne podmioty uczestniczące w przetwarzaniu danych, których dotyczy naruszenie (*opcjonalnie, np. podmiot przetwarzający, współadministratora, operator pocztowy itp.*): …

7. Informacje na temat naruszenia ujawnione w toku czynności sprawdzających:

Data i miejsce naruszenia

…

Kategorie osób, których danych dotyczy naruszenie

☐ potencjalnych pracowników

☐ pracowników / współpracowników

☐ dostawców

☐ kontrahentów

☐ innych osób (*należy określić jakie to osoby*): …

Kategorie danych osobowych, których dotyczy naruszenie

1) Dane osobowe *zwykłe*

☐ imię

☐ nazwisko

☐ numer telefonu

☐ adres mailowy

☐ adres zamieszkania

☐ adres zameldowania

☐ adres korespondencyjny

☐ PESEL

☐ NIP

☐ inne dane (*należy określić jakie to kategorie danych)*: …

2) Szczególne kategorie danych osobowych

☐ pochodzenie rasowe lub etniczne

☐ poglądy polityczne

☐ przekonania religijne lub światopoglądowe

☐ przynależność do związków zawodowych

☐ dane genetyczne

☐ dane biometryczne

☐ dane dotyczące zdrowia

☐ seksualność lub orientację seksualną

3) Kategorie danych osobowych podlegające szczególnej ochronie

☐ wyroki skazujące

☐ czyny zabronione lub powiązane środki bezpieczeństwa

Przybliżona liczba osób, których dotyczy naruszenie:

…

Przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie:

…

Opis naruszenia:

…

Naruszenie polegało na:

☐ zgubienie lub kradzież nośnika/urządzenia

☐ dokumentacja papierowa (zawierająca dane osobowe) zgubiona, skradziona lub pozostawiona w niezabezpieczonej lokalizacji

☐ korespondencja papierowa utracona przez operatora pocztowego lub otwarta przed zwróceniem jej do nadawcy

☐ nieuprawnione uzyskanie dostępu do informacji

☐ nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń

☐ złośliwe oprogramowanie ingerujące w poufność, integralność lub dostępność danych

☐ uzyskanie poufnych informacji przez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, takiej jak e-mail czy komunikator internetowy (phishing)

☐ nieprawidłowa anonimizacja danych osobowych w dokumencie

☐ nieprawidłowe usunięcie/zniszczenie danych osobowych z nośnika/urządzenia elektronicznego przed jego zbyciem przez administratora

☐ niezamierzona publikacja

☐ dane osobowe wysłane do niewłaściwego odbiorcy

☐ ujawnienie danych niewłaściwej osoby

☐ ustne ujawnienie danych osobowych

Charakter naruszenia:

☐ naruszenie dotyczące poufności danych

**dochodzi do nieuprawnionego lub przypadkowego ujawnienia lub nieuprawnionego dostępu do danych osobowych*

☐ naruszenie dotyczące integralności danych

**dochodzi do nieuprawnionego lub przypadkowego zmodyfikowania danych osobowych*

☐ naruszenie dotyczące dostępności danych

**dochodzi do przypadkowego lub nieuprawnionego dostępu do danych osobowych lub zniszczenia danych osobowych*

7. Przyczyna naruszenia

☐ wewnętrzne działanie niezamierzone

☐ wewnętrzne działanie zamierzone

☐ zewnętrzne działanie niezamierzone

☐ zewnętrzne działanie zamierzone

8. Ocena naruszenia

Ocena ryzyka z kalkulacji

☐ brak ryzyka

☐ ryzyko

☐ wysokie ryzyko

Końcowa ocena

Naruszenie kwalifikowane jest jako:

☐ nieskutkujące ryzykiem naruszenia praw lub wolności osób fizycznych

☐ skutkujące ryzykiem naruszenia praw lub wolności osób fizycznych

☐ skutkujące wysokim ryzykiem naruszenia praw lub wolności osób fizycznych

Uzasadnienie

…

9. Powiadomienie organu nadzorczego

Naruszenie kwalifikowane jest jako:

☐ niewymagające powiadomienia organu nadzorczego

☐ wymagające powiadomienia organu nadzorczego

10. Zawiadomienie osoby, której dane dotyczą

Naruszenie kwalifikowane jest jako:

☐ niewymagające zawiadomienia osoby, której dane dotyczą

☐ wymagające zawiadomienia osoby, której dane dotyczą

11. Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa dotychczas stosowanych

…

12. Środki bezpieczeństwa zastosowane lub proponowane w celu zminimalizowana ryzyka ponownego wystąpienia naruszenia

…

13. Środki zastosowane lub proponowane w celu zaradzenia naruszeniu i zminimalizowania negatywnych skutków dla osób, których dane dotyczą

…

14. Załączniki:

Załącznik nr 1 – *Kalkulacja oceny ryzyka naruszenia*

.....

Data i podpis OBDO

Otrzymują:

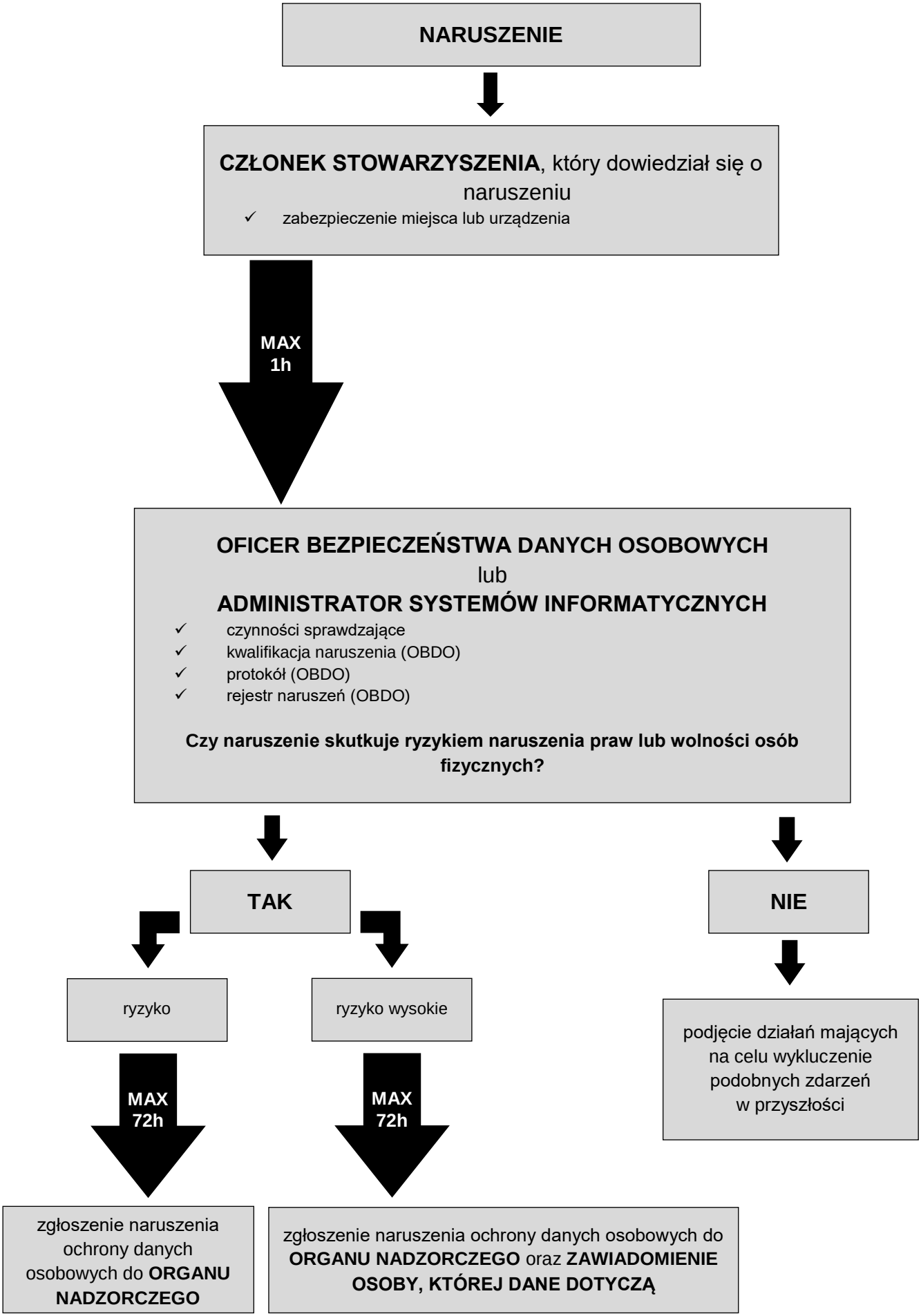
1 x oryginał Administrator Danych

1 x kopia OBDO

Wzór rejestru naruszeń ochrony danych osobowych

Lp.	Numer naruszenia	Data i miejsce naruszenia *(dd/mm/rrrr, miejsce)*	Opis naruszenia *(krótki opis naruszenia, w szczególności poprzez odesłanie do sporządzonego Protokołu z naruszenia ochrony danych osobowych)*	Kwalifikacja naruszenia	Zawiadomienie organu nadzorczego *(tak / nie)*	Zawiadomienie osób, których dane dotyczą *(tak / nie)*
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						

Schemat graficzny procedury



OCENA RYZYKA NARUSZENIA				
LP.	**KRYTERIUM**		**OCENA**	**UZASADNIENIE**
1.	**Charakter i wrażliwość danych** **należy określić, czy dane osobowe, których dotyczy naruszenie mają szczególne znaczenie dla osoby, której dane dotyczą, a ich ujawnienie niesie za sobą poważne konsekwencje* ** np.: dane związane z życiem zawodowym (mniej wrażliwe), dane związane z życiem prywatnym (bardziej wrażliwe), EROD: "ujawnienie imienia i nazwiska oraz adresu danej osoby prawdopodobnie nie wyrządzi jej szkody w normalnej sytuacji. Jednak jeżeli imię i nazwisko oraz adres rodzica adopcyjnego zostaną ujawnione rodzicowi biologicznemu, może mieć to bardzo poważne konsekwencje zarówno dla rodzica adopcyjnego, jak i dziecka"*			
2.	**Rodzaj danych** **należy ocenić rodzaj danych osobowych, których dotyczy naruszenie, także w kontekście kategorii danych osobowych*	dane zwykłe		
		szczególne kategorie danych osobowych		
		dane dotyczące wyroków skazujących i czynów zabronionych		
3.	**Łatwość identyfikacji osoby** **należy ocenić czy osoba / podmiot, który wszedł w posiadanie danych osobowych będzie w stanie dokonać identyfikacji osoby, której dane dotyczą*			
4.	**Konsekwencje** **należy zidentyfikować jakie są konsekwencje naruszenia dla osoby, której dane dotyczą*	Utrata kontroli nad własnymi danymi osobowymi		
		Ograniczenie możliwości realizowania praw z art. 15-22 RODO		

Ograniczenie możliwości realizowania praw		
Dyskryminacja		
Kradzież lub sfałszowanie tożsamości		
Strata finansowa		
Naruszenie dobrego imienia		
Utrata poufności danych osobowych chronionych tajemnicą zawodową		
Nieuprawnione odwrócenie pseudonimizacji		
Niemożliwość świadczenia usługi / realizacji umowy		
inne **jeżeli występują konsekwencje inne niż wskazane powyżej, należy je dodatkowo zidentyfikować*		
inne **jeżeli występują konsekwencje inne niż wskazane powyżej, należy je dodatkowo zidentyfikować*		

		inne **jeżeli występują konsekwencje inne niż wskazane powyżej, należy je dodatkowo zidentyfikować*		
		inne **jeżeli występują konsekwencje inne niż wskazane powyżej, należy je dodatkowo zidentyfikować*		
		inne **jeżeli występują konsekwencje inne niż wskazane powyżej, należy je dodatkowo zidentyfikować*		
		inne **jeżeli występują konsekwencje inne niż wskazane powyżej, należy je dodatkowo zidentyfikować*		
5.	**Podmiot niezaufany** ** należy określić czy podmiot, który uzyskał / mógł uzyskać dostęp do danych osobowych jest podmiotem niezaufanym (tj. innym niż zaufany)* **podmiot zaufany to taki, z którym Administrator Danych pozostaje w stałych stosunkach, może znać stosowane u niego procedury, historię, inne szczegóły go dotyczące np. podmiot przetwarzający, z którym mamy podpisaną umowę powierzenia przetwarzania danych osobowych*			
6.	**Cechy szczególne osoby** **należy wziąć pod uwagę czy osoby, których danych osobowych dotyczy naruszenie należą do grup osób wymagających szczególnej opieki i / lub można stwierdzić brak równowagi między stanowiskiem osoby, której dane dotyczą, a stanowiskiem Administratora Danych*	osoby starsze (pow. 60 r.ż.)		
		dzieci (pon. 16 r.ż.)		
		osoby niepełnosprawne		
		inne **jeżeli występują grupy inne niż wskazane powyżej, należy je dodatkowo zidentyfikować*		

		inne **jeżeli występują grupy inne niż wskazane powyżej, należy je dodatkowo zidentyfikować*		
		inne **jeżeli występują grupy inne niż wskazane powyżej, należy je dodatkowo zidentyfikować*		
7.	**Brak publicznej dostępności danych** **należy określić czy dane osobowe, których dotyczy naruszenie nie są dostępne w ogólnodostępnych źródłach informacji np. CEIDG, portale społecznościowe, KRS, strony internetowe*			
8.	**Aktualność danych** **należy określić czy dane osobowe, których dotyczy naruszenie są aktualne oraz poprawne merytorycznie*			

WYNIK KALKULACJI

**niezależnie od wyniku kalkulacji, końcowa ocena naruszenia może się od niego różnić ze względu na dodatkowe czynniki (podnoszące lub obniżające ryzyko) brane pod uwagę przy ustalaniu oceny końcowej naruszenia stanowiącej część Protokołu z naruszenia ochrony danych osobowych*

Brak ryzyka (do 19%)
Ryzyko (20%-49%)
Ryzyko wysokie (50%-100%)

Załącznik nr 6A – Procedura oceny ryzyka dla procesów lub sposobów organizacji przetwarzania danych osobowych

1. Administrator Danych jest odpowiedzialny za zapewnienie przeprowadzenia oceny ryzyka dla procesów lub sposobów organizacji przetwarzania danych osobowych.
2. OBDO na podstawie swojej wiedzy oraz informacji przekazanych mu przez Osoby zarządzające procesami przetwarzania danych osobowych oraz innych pracowników Administratora Danych przetwarzających dane osobowe, wydaje rekomendacje co do procesów lub sposobów organizacji przetwarzania danych osobowych wymagających przeprowadzenia oceny ryzyka. Wydana przez OBDO rekomendacja przekazywana jest do Administratora Danych.
3. Administrator Danych podejmuje ostateczną decyzję o przeprowadzeniu lub nieprzeprowadzeniu oceny ryzyka dla danego procesu lub sposobu organizacji przetwarzania danych osobowych.
4. Za właściwą koordynację oceny ryzyka odpowiada OBDO.
5. W ocenie ryzyka biorą udział pracownicy Administratora Danych, którzy posiadają szczegółową wiedzę na temat procesu lub sposobu organizacji przetwarzania danych osobowych, która podlega ocenie.
6. Ocena ryzyka przeprowadzana jest przy wykorzystaniu matrycy, której wzór stanowi Załącznik nr 6B do Polityki.
7. Ocena ryzyka składa się z czterech etapów:
    7.1. Etap 1 – ustalanie kontekstu dla procesu lub sposobu organizacji przetwarzania danych osobowych, tj. określenie zaangażowanych aktywów,
    7.2. Etap 2 – ustalanie mechanizmów kontrolnych, tj. wskazanie zabezpieczeń stosowanych w kontekście każdego ze zdefiniowanych aktywów,
    7.3. Etap 3 – szacowanie ryzyka, tj. określenie prawdopodobieństwa wystąpienia zagrożenia będącego naruszeniem praw lub wolności osób fizycznych, których dane dotyczą, co następuje na podstawie zdefiniowanych w Etapie 2 zabezpieczeń,
    7.4. Etap 4 – działania zapobiegawcze i korygujące, tj. wskazanie środków naprawczych, w kontekście zagrożeń, w odniesieniu do których występuje prawdopodobieństwo ich urzeczywistnienia.
8. Podczas Etapu 3, tj. szacowania ryzyka, uwzględnia się:
    8.1. wagę zdefiniowanego zagrożenia, tj. wielkości szkody, jakie zdarzenie to może spowodować w odniesieniu do osoby, której dane dotyczą,
    8.2. prawdopodobieństwa wystąpienia określonego zagrożenia będącego naruszeniem.
9. Ryzyko należy oszacować na podstawie obiektywnej i rzeczowej analizy, w ramach której stwierdza się, czy z procesem lub sposobem organizacji przetwarzania danych osobowych wiąże się ryzyko i jaki jest jego stopień.

10. Końcowym wynikiem oceny ryzyka naruszenia praw i wolności osób, których dane dotyczą, jest określenie poziomu ryzyka dla danego procesu lub sposobu organizacji przetwarzania danych osobowych. Poziom ryzyka określa się jako:

    10.1. brak ryzyka,

    10.2. niski,

    10.3. średni,

    10.4. wysoki.

11. OBDO przedkłada przeprowadzoną ocenę ryzyka Administratorowi Danych.

12. Jeżeli w wyniku oceny ryzyka zostało stwierdzone ryzyko naruszenia praw lub wolności osób fizycznych, Administrator Danych, na podstawie przedłożonej mu oceny, podejmuje ostateczną decyzję w zakresie postępowania z tym ryzykiem. W szczególności, decyzja ta może polegać na zarządzeniu:

    12.1. modyfikacji (redukcji) ryzyka –. obniżenie poziomu ryzyka poprzez realizację określonych w Etapie 4 działań zapobiegawczych i korygujących,

    12.2. zachowania (akceptacji) ryzyka – świadoma i obiektywna decyzja o niewprowadzaniu żadnych zmian w procesie lub sposobie organizacji przetwarzania danych osobowych, pomimo stwierdzonego ryzyka,

    12.3. unikania ryzyka – unikanie działań, które powodują powstanie określonych zagrożeń, co może wiązać się z koniecznością rezygnacji z danego procesu lub sposobu organizacji przetwarzania danych osobowych,

    12.4. dzielenia (przeniesienia) ryzyka – wykupienie ubezpieczenia lub scedowanie skutków ryzyka na inny podmiot, co nie będzie stanowiło eliminacji ryzyka niezastosowania się przez Administratora Danych do przepisów RODO.

13. OBDO koordynuje wdrożenie działań, o których mowa w pkt 12.1 powyżej.

14. Szacowanie ryzyka należy traktować jako proces ciągły, a ochrona danych osobowych powinna być zapewniona na każdym etapie procesu przetwarzania danych i na każdym etapie funkcjonowania wdrożonego w strukturach Administratora Danych systemu przetwarzania danych osobowych.

OCENA RYZYKA		Wskazówki metodologiczne
Administrator Danych **nazwa, siedziba*		*należy zidentyfikować Administratora Danych*
Data **dd/mm/rrr*		*należy podać datę zakończenia przeprowadzenia oceny*
Nazwa procesu lub sposobu organizacji podlegającego ocenie		*należy określić proces lub sposób organizacji przetwarzania danych osobowych, które podlegają ocenie ryzyka (np. praca zdalna, wykorzystywanie prywatnego sprzętu dla celów służbowych, monitoring wizyjny na terenie zakładu Administratora Danych)*
Osoby biorące udział w ocenie **Należy wskazać imiona, nazwiska oraz stanowiska osób biorących udział w ocenie oraz wskazać ich rola w w zakresie przeprowadzanej oceny*		*należy wskazać osoby biorące udział w ocenie ryzyka oraz określić ich rolę, w szczególności poprzez wskazanie obszaru, w ramach którego udzielali oni informacji (np. Jan Kowalski, Dyrektor Działu HR, wskazanie zabezpieczeń organizacyjnych odmawiających się do użytkownika), udział w określeniu prawdopodobieństwa wystąpienia zagrożenia dla kategorii zagrożenia użytkownik)*
Ogólny opis przetwarzania danych osobowych w ramach procesu lub sposobu organizacji przetwarzania danych osobowych **Należy zidentyfikować przetwarzanie danych osobowych (m.in. poprzez wskazanie na czym polega, jaki jest jego cel, czy jego wdrożenie podyktowane jest potrzebą biznesową, etc.) oraz wskazać jego cel.*		*należy dokonać identyfikacji procesu lub sposobu przetwarzania danych osobowych podlegającego ocenie ryzyka, w szczególności poprzez odniesienie się do celów wdrożenia rozwiązania, jaki jest jego cel, na czym polega, jakie są etapy wdrożenia, a jeżeli przetwarzanie już się odbywa, czym jest to spowodowane i jak wyglądało to wdrożenie, ajeli powinien odnosić się w szczególności do przetwarzania danych osobowych i uwzględniać w sobie wszelkie czynniki związane z tym przetwarzaniem*
Kategorie osób, których dane dotyczą **Należy wskazać czyje dane osobowe będą przetwarzane*		*należy określić kogo dane osobowe są przetwarzane w procesie lub sposobie organizacji przetwarzania danych osobowych podlegającego ocenie, kategorie osób powinny zostać wyliczone w sposób kompletny, mogłyby w sposób najbardziej szczegółowy (np., kandydaci do pracy, pracownicy, byli pracownicy, kontrahenci, osoby objęte monitoringiem wizyjnym, etc.)*
Zakres danych osobowych przetwarzanych w ramach procesu lub sposobu organizacji przetwarzania danych osobowych podlegającego szacowaniu ryzyka **Należy wskazać jakie dane osobowe są przetwarzane oraz czy przetwarzane są / będą szczegółne kategorie danych osobowych lub dane osobowe dotyczące wyroków skazujących i czynów zabronionych*		*należy określić jakie dane osobowe są przetwarzane w procesie lub sposobie organizacji przetwarzania danych osobowych podlegającego ocenie, kategorie danych powinny zostać wyliczone w sposób jak najbardziej szczegółowy, z uwzględnieniem szczególnych kategorii danych osobowych oraz danych podlegających szczególnym warunkom przetwarzania (określenie poprzez szczególnie wyliczenie tj. np. imię, nazwisko, dane kontaktowe:numer telefonu, adres email) lub poprzez posługiwanie się sześcioma określeniami tj. np. dane identyfikacyjne, dane kontaktowe, dane finansowe)*
Skala przetwarzania **Należy określić jaka jest skala przetwarzania danych*		*należy określić jaka jest skala przetwarzania danych osobowych w procesie lub sposobie organizacji przetwarzania danych osobowych podlegającego ocenie ryzyka, skalę należy ocenić w odniesieniu do działalności konkretnego Administratora Danych, w tym zakresie można posłużyć się wyliczeniem procentowym, wskazując jaki procent z wszystkich danych osobowych przetwarzanych przez Administratora Danych występuje w procesie lub sposobie przetwarzania*
Retencja **Należy określić szacunkowy czas przetwarzania danych osobowych w ramach przetwarzania podlegającego szacowaniu ryzyka*		*należy określić jaki czas przetwarzania dla danych osobowych przetwarzanych w procesie lub sposobie organizacji przetwarzania danych osobowych podlegającego ocenie ryzyka, w szczególności w tym zakresie należy uwzględnić projekte terminy retencji dla poszczególnych danych osobowych*

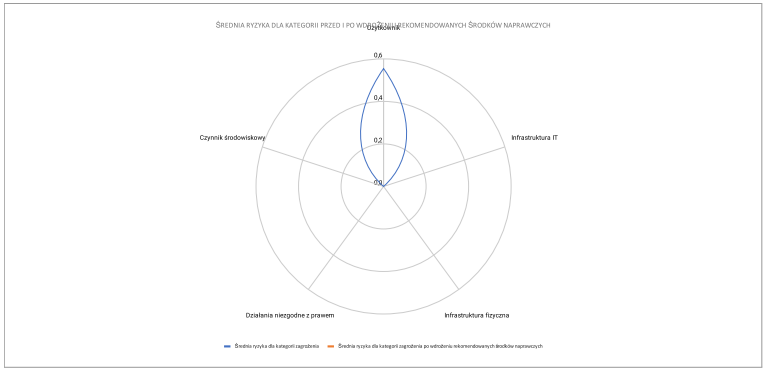
Ustalanie kontekstu (ETAP 1)			Ustalanie mechanizmów kontrolnych (ETAP 2)			ETAP 1 - należy określić jakie aktywa (zasoby wymierzonych) występują w danym procesie lub sposobie organizacji przetwarzania danych osobowych podlegającego ocenie ryzyka, jeżeli dany rodzaj aktywa nie występuje, należy oznaczyć odpowiednią odpowiedź, w takim wypadku, ETAP 2 dla danego rodzaju aktywa nie jest realizowany. ETAP 2 - dla każdego z rodzajów aktywów należy określić sposoby jego zabezpieczeń, z podziałem na organizacyjne, techniczne i fizyczne, zabezpieczenia te powinny zostać opisane w sposób jak możliwie najbardziej szczegółowy, odbytenie w tym zakresie do konkretnych regułoj wewnętrznych będzie możliwe jedynie wówczas, kiedy regulacje te są aktualne i wskazują na faktycznie stosowane środki zabezpieczeń.
Lp.	**Kategoria aktywów**	**Czy to aktywa ADO?**	**Zabezpieczenia organizacyjne**	**Zabezpieczenia techniczne**	**Zabezpieczenia fizyczne**	
1.	Użytkownicy					
2.	Sprzęt					
3.	Oprogramowanie					
4.	Sieci i przesyłanie danych					
5.	Dane w formie papierowej					
6.	Lokalizacja					

Szacowanie ryzyka (ETAP 3)									Działania zapobiegawcze i korygujące (ETAP 4)				ETAP 3 - na podstawie wskazanych w ETAPIE 2 zabezpieczeń, należy określić prawdopodobieństwo wystąpienia danego zagrożenia, które przyjęto dla określenia prawdopodobieństwa zostało wskazana na dole formularza, dla każdej wskazanej kategorii zagrożenia, szacowanie prawdopodobieństwa powinno nastąpować z uwzględnieniem wszystkich aktywów i ich zabezpieczeń wskazanych w ETAPIE 1 oraz ETAPIE 2, jeżeli pojawia się wątpliwości przy określeniu prawdopodobieństwa, należy przyjąć wartość większą, ryzyko oraz średnia ryzyka dla danej kategorii zagrożenia wyliczane są automatycznie, waga danego zagrożenia przyjęta została na sztywno i nie powinna podlegać modyfikacjom ETAP 4 - jeżeli pojawia się ryzyko wystąpienia danego rodzaju zagrożenia, należy wskazać środki naprawcze, które rekomenduje się, aby wdrożyć, by ryzyko to zniwelować lub obniżyć, jeżeli ryzyka takie nie występuje lub brak jest środków, które mogłyby obniżyć występujące ryzyko, należy wpisać wartość prawdopodobieństwa taką samą jak w ETAPIE 3, w innym wypadku wynik oceny końcowej może zostać obliczony niepoprawiłowo, ryzyko oraz średnia ryzyka dla danej kategorii zagrożenia po wdrożeniu rekomendowanych środków wyliczane są automatycznie
Lp.	**Kategoria zagrożenia**	**Zagrożenie**	**w zagrożenia na dane osob**	**Waga**	**Prawdopodobieństwo**	**Uzasadnienie dla wskazanego prawdopodobieństwa**	**Ryzyko**	**Średnia ryzyka dla kategorii zagrożenia**	**Rekomendowane środki naprawcze**	**Prawdopodobieństwo po wdrożeniu rekomendowanych środków naprawczych**	**Ryzyko po wdrożeniu rekomendowanych środków naprawczych**	**Średnia ryzyka dla kategorii zagrożenia po wdrożeniu rekomendowanych środków naprawczych**	
1.	**Użytkownik**	używanie sprzętu w celach prywatnych	utrata kontroli łączenie z informacjami prywatnymi dostęp osoby nieupoważnionej nieuprawniona ingerencja /	3	2		3	0,6			0	0,0	
2.		używanie prywatnych nośników danych	utrata kontroli łączenie z informacjami prywatnymi dostęp osoby nieupoważnionej	3			0				0		
3.		nieużywanie haseł	dostęp osoby nieupoważnionej	3	1		2				0		
4.		używanie zbyt prostych haseł	dostęp osoby nieupoważnionej	2			0				0		
5.		brak znajomości procedur	przetwarzanie niezgodne z prawem przetwarzanie niezgodne z procedurami	2			0				0		
6.		brak nadzoru nad nośnikiem danych (sprzęt / dokumenty papierowe)	dostęp osoby nieupoważnionej utrata	3			0				0		
7.		współdzielenie sprzętu z wieloma osobami	utrata kontroli łączenie z informacjami prywatnymi łączenie z informacjami dotyczącymi innych osób dostęp osoby	3			0				0		
8.		zgubienie nośnika danych	utrata	3			0				0		
9.		narażenie nośnika danych na uszkodzenie środowiskowe (spalenie / zalanie / wilgoć / pył / temperaturę)	zniszczenie	3			0				0		
10.	**Infrastruktura IT**	awaria stacji roboczej (sprzęt)	utrata dostępu utrata	2			0	0,0			0	0,0	
11.		awaria stacji roboczej (oprogramowanie)	utrata dostępu utrata	2			0				0		
12.		awaria serwera (sprzęt)	utrata dostępu utrata	2			0				0		
13.		awaria serwera (oprogramowanie)	utrata dostępu utrata	2			0				0		
14.		awaria infrastruktury sieciowej (połączeń sieciowych)	utrata dostępu utrata	2			0				0		
15.		awaria dostępu do Internetu	utrata dostępu utrata	2			0				0		
16.		awaria zasilania stacji roboczej	utrata dostępu utrata	2			0				0		
17.		awaria zasilania serwera	utrata dostępu utrata	2			0				0		
18.		awaria UPS stacji roboczej	utrata dostępu utrata	2			0				0		
19.		awaria UPS serwera	utrata dostępu utrata	2			0				0		
20.		awaria systemu chłodzenia (sprzęt)	utrata dostępu utrata	2			0				0		
21.		awaria systemu chłodzenia (serwer)	utrata dostępu utrata	2			0				0		
22.		błąd oprogramowania systemowego	utrata dostępu utrata modyfikacja	3			0				0		
23.		błąd oprogramowania specjalistycznego	utrata dostępu utrata modyfikacja	3			0				0		
24.		brak wykonywanych kopii danych	utrata	2			0				0		
25.		brak obsługi informatycznej	utrata	2			0				0		
26.	**Infrastruktura fizyczna**	brak niezbędnej infrastruktury służącej do przetwarzania danych (szafy / niszczarki / zamykane pomieszczenia)	utrata kontroli dostęp osoby nieupoważnionej przypadkowe zniszczenie /	3			0	0,0			0	0	

27.	Działania niezgodne z prawem	skuteczny atak hakera	utrata kontroli dostęp osoby nieupoważnionej niezgodne z prawem zniszczenie / utrata / modyfikacja niezgodne z prawem wykorzystanie	3			0	0,0			0	0,0
28.		skuteczny phishing	utrata kontroli dostęp osoby nieupoważnionej niezgodne z prawem zniszczenie / utrata / modyfikacja niezgodne z prawem wykorzystanie	3			0				0	
29.		kradzież	utrata kontroli dostęp osoby nieupoważnionej niezgodne z prawem zniszczenie / utrata / modyfikacja niezgodne z prawem wykorzystanie	3			0				0	
30.		włamanie	utrata kontroli dostęp osoby nieupoważnionej niezgodne z prawem zniszczenie / utrata / modyfikacja niezgodne z prawem wykorzystanie	3			0				0	
31.		uzyskanie dostępu osoby nieupoważnionej do stacji roboczej (dostęp logiczny)	utrata kontroli dostęp osoby nieupoważnionej niezgodne z prawem zniszczenie / utrata / modyfikacja niezgodne z prawem wykorzystanie	3			0				0	
32.		uzyskanie dostępu osoby nieupoważnionej do serwera (dostęp logiczny)	utrata kontroli dostęp osoby nieupoważnionej niezgodne z prawem zniszczenie / utrata / modyfikacja niezgodne z prawem wykorzystanie	3			0				0	
33.		uzyskanie dostępu osoby nieupoważnionej do dokumentów papierowych (dostęp fizyczny)	utrata kontroli dostęp osoby nieupoważnionej niezgodne z prawem zniszczenie / utrata / modyfikacja niezgodne z prawem wykorzystanie	3			0				0	
34.	Czynnik środowiskowy	pożar	zniszczenie	2			0	0,0			0	0,0
35.		powódź	zniszczenie	2			0				0	
36.		zalanie	zniszczenie	2			0				0	
37.		uszkodzenie spowodowane przez burze (pioruny)	zniszczenie	2			0				0	

OCENA KOŃCOWA	Obecnie	Po wdrożeniu rekomendowanych środków naprawczych
Suma wartości ryzyk dla zagrożeń	5	0
Przetwarzanie szczególnych kategorii danych osobowych	0	0
Przetwarzanie danych szczególnych kategorii osób *np. dzieci, osoby starsze, osoby niepełnosprawne*	0	0
SUMA **końcowa suma wartości ryzyk z obszarów oraz dodatkowych ryzyk*	**5**	**0**
POZIOM RYZYKA	Niski	Brak
Uzasadnienie:		

końcowa wartość ryzyk oraz końcowa suma ryzyk, o takim poziom ryzyka wyliczane są automatycznie na podstawie wskazanych w ETAPIE 3 i 4 prawdopodobieństw
suma wartości ryzyk może zostać ręcznie podniesiona, w związku z dodatkowym uwzględnieniem przetwarzania szczególnych kategorii danych osobowych lub danych osobowych dotyczących szczególnych kategorii osób (podniesienie sumy następuje wówczas o 1, 2 lub 3 punkty), w zależności od ostatecznej oceny osoby dokonującej oceny ryzyka
ocenę końcową należy uzasadnić poprzez wskazanie czynników, które się na nią złożyły, w szczególności poprzez wskazanie zagrożeń, które mają szczególny wpływ na ostateczną ocenę ryzyka dla procesu lub sposobu organizacji przetwarzania danych osobowych
wykres obrazuje jak może zmienić się ryzyka po wdrożeniu rekomendowanych środków naprawczych



WZÓR WYLICZENIA RYZYKA					SZACOWANIE PRAWDOPODOBIEŃSTWA
waga 3	0	2	3	3	0 - brak ało prawdopodobne rankowanie możliwe oce prawdopodobne
waga 2	0	1	2	3	
waga 1	0	1	1	2	
waga 0	0	0	0	0	
	0	1	2	3	
	prawdopodobieństwo				

UWAGA!
Poziom ryzyka ustala się w zależności od SUMY, tj.:
0 - brak
1-30 - niski
31-70 - średni
71-111 - wysoki

Kategorie	Średnia ryzyka dla kategorii zagrożenia	Średnia ryzyka dla kategorii zagrożenia po wdrożeniu rekomendowanych środków naprawczych
Użytkownik	0,6	0,0
Infrastruktura IT	0,0	0,0
Infrastruktura fizyczna	0,0	0,0
Działania niezgodne z prawem	0,0	0,0
Czynnik środowiskowy	0,0	0,0

Załącznik nr 7A – Procedura oceny skutków dla ochrony danych osobowych (*data protection impact assessment*)

1. Administrator Danych jest odpowiedzialny za zapewnienie przeprowadzenia oceny skutków dla ochrony danych osobowych (*data protection impact assessment*).
2. Za właściwą koordynację DPIA odpowiada OBDO.
3. Przeprowadzenie DPIA jest obowiązkowe zawsze, gdy:
   3.1. dany rodzaj przetwarzania został wskazany w wykazie ustanowionym przez organ nadzorczy jako podlegający wymogowi dokonana oceny,
   3.2. ze względu na swój charakter, zakres, kontekst i cele, przetwarzanie danych może z dużym prawdopodobieństwem powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.
4. OBDO dokonuje analizy, czy dany rodzaj operacji będzie podlegał obowiązkowi przeprowadzenia DPIA.
5. Analizie poddawany jest każda operacja (proces) przetwarzania danych osobowych ujawniona w rejestrze czynności przetwarzania Administratora Danych. Odbywa się to zgodnie z Załącznikiem nr 7B do Polityki.
6. Niezależnie od powyższego, analizie może zostać poddana każda inna operacja przetwarzania danych osobowych, w tym w szczególności operacja planowana. Taka analiza odbywa się zgodnie z szablonem Analizy planowanej operacji przetwarzania, której wzór znajduje się w niniejszym Załączniku.
7. Osoba zarządzająca procesami przetwarzania danych osobowych jest zobowiązana do poinformowania OBDO o planowanym wdrożeniu nowej operacji przetwarzania oraz planowanych zmianach w trwającej operacji przetwarzania.
8. Osoba zarządzająca procesami przetwarzania danych osobowych przekazuje OBDO szczegółowe informacje dotyczące operacji poddawanej analizie.
9. W razie konieczności, w toku prowadzonej analizy, OBDO konsultuje się z Osobą zarządzającą procesami przetwarzania danych osobowych. W tym zakresie, Osoba zarządzająca procesami przetwarzania danych osobowych jest zobowiązana udzielić OBDO wszelkich niezbędnych informacji na temat operacji podlegającej analizie, o której mowa w pkt 4.
10. Jeżeli w toku dokonywania analizy, OBDO wskaże, że dany rodzaj operacji przetwarzania został ujawniony w wykazie ustanowionym przez organ nadzorczy jako podlegający wymogowi dokonana oceny, DPIA dla tej operacji przetwarzania przeprowadzana jest obowiązkowo.
11. W przypadkach innych niż wskazane w pkt 10, OBDO weryfikuje, czy dany rodzaj operacji może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. W tym zakresie OBDO bierze pod uwagę, w szczególności, czy planowana operacja wiąże się z:

11.1. dokonywaniem ocen lub punktacji,

11.2. zautomatyzowanym podejmowaniem decyzji o skutku prawnym lub podobnie znaczącym skutku,

11.3. systematycznym monitorowaniem,

11.4. przetwarzaniem szczególnych kategorii danych lub danych osobowych podlegających szczególnym warunkom przetwarzania,

11.5. przetwarzaniem danych osobowych na dużą skalę,

11.6. dopasowywaniem lub łączeniem zbiorów danych,

11.7. przetwarzaniem danych dotyczącym osób wymagających szczególnej opieki,

11.8. innowacyjnym wykorzystaniem lub stosowaniem nowych rozwiązań technologicznych lub organizacyjnych,

11.9. przetwarzaniem uniemożliwiającym osobom, których dane dotyczą, wykonywanie praw, korzystanie z usługi lub realizację umowy.

12. Za operacje mogące powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych uważa się, w szczególności operacje, które spełniają co najmniej dwa ze wskazanych w pkt 11 kryteriów. W niektórych przypadkach, OBDO może jednak uznać, że:

12.1. przetwarzanie spełniające tylko jedno z kryteriów będzie wymagało przeprowadzenia oceny,

12.2. przetwarzanie spełniające dwa lub więcej kryteriów nie będzie wymagało przeprowadzenia oceny.

13. We wskazanych w pkt 12.1 i pkt 12.2 przypadkach, OBDO szczegółowo uzasadnia swoje stanowisko, w szczególności powołując się na decyzje organów nadzorczych, wytyczne Europejskiej Rady Ochrony Danych, orzecznictwo, praktykę doktryny lub na własne doświadczenia w tym zakresie.

14. Administrator Danych podejmuje ostateczną decyzję o przeprowadzeniu lub nieprzeprowadzeniu DPIA dla danej operacji przetwarzania i informuje o tym OBDO.

15. OBOD oraz Osoba zarządzająca procesami przetwarzania danych osobowych opracowują wspólnie harmonogram przeprowadzenia DPIA, który wskazuje, w szczególności na:

17.1. osoby uczestniczące w dokonywaniu oceny,

17.2. datę rozpoczęcia oceny,

17.3. przewidywaną datę zakończenia oceny.

16. Dokonując oceny uwzględnia się co najmniej:

18.1. opis procesu przetwarzania danych osobowych (operacja i cele przetwarzania, a jeżeli ma to zastosowanie również prawnie usprawiedliwione interesy realizowane przez Administratora Danych),

18.2. ocenę niezbędności i proporcjonalności tego przetwarzania

18.3. ocenę ryzyka naruszenia praw lub wolności osób fizycznych,

18.4. wykaz środków, mających zaradzić ewentualnie stwierdzonemu ryzyku (zabezpieczenia oraz środki i mechanizmy bezpieczeństwa).

17. W przypadku, jeśli przetwarzanie danych osobowych dokonywane jest przy udziale podmiotu przetwarzającego, podmiot ten powinien uczestniczyć w przeprowadzeniu oceny skutków dla ochrony danych oraz udzielać niezbędnych informacji.

18. W sytuacji, w której operacja przetwarzania dotyczy współadministratorów, ich obowiązki powinny zostać dokładnie określone i rozdzielone. DPIA powinna jasno wskazywać, która strona jest odpowiedzialna za stosowanie odpowiednich środków przewidzianych do zaradzenia ryzyku oraz ochrony praw osób, których dane dotyczą.

19. Po przeprowadzeniu DPIA, OBDO przedkłada Administratorowi Danych Raport z przeprowadzonej oceny skutków dla ochrony danych osobowych zgodny z wzorem znajdującym się w niniejszym Załączniku.

20. Jeżeli w wyniku oceny zostało stwierdzone prawdopodobieństwo wystąpienia ryzyka naruszenia praw lub wolności osób fizycznych, Administrator Danych na podstawie przedłożonego mu Raportu z oceny skutków dla ochrony danych osobowych, podejmuje ostateczną decyzję w zakresie realizacji określonego Planu naprawczego. W szczególności, dotyczy to akceptacji wskazanych w Planie naprawczym środków, które powinny zostać podjęte w celu zaradzenia stwierdzonemu ryzyku bądź jego zminimalizowaniu.

21. Na podstawie Planu naprawczego zatwierdzonego przez Administratora Danych, OBDO oraz Osoba zarządzająca procesami przetwarzania danych osobowych ustalają harmonogram wdrożeń środków wskazanych w Planie naprawczym.

22. W sytuacji, w której przeprowadzona ocena wykaże, że przetwarzanie danych powodowałoby wysokie ryzyko, gdyby Administrator Danych nie zastosował środków w celu zminimalizowania ryzyka, przed rozpoczęciem przetwarzania, Administrator Danych konsultuje się z organem nadzorczym w trybie art. 36 RODO.

23. Konsultując się z organem nadzorczym Administrator Danych przedstawia mu:

26.1. gdy ma to zastosowanie – odpowiednie obowiązki Administratora Danych, współadministratorów oraz podmiotów przetwarzających uczestniczących w przetwarzaniu,

26.2. cele i sposoby zamierzonego przetwarzania,

26.3. środki i zabezpieczenia mające chronić prawa i wolności osób, których dane dotyczą,

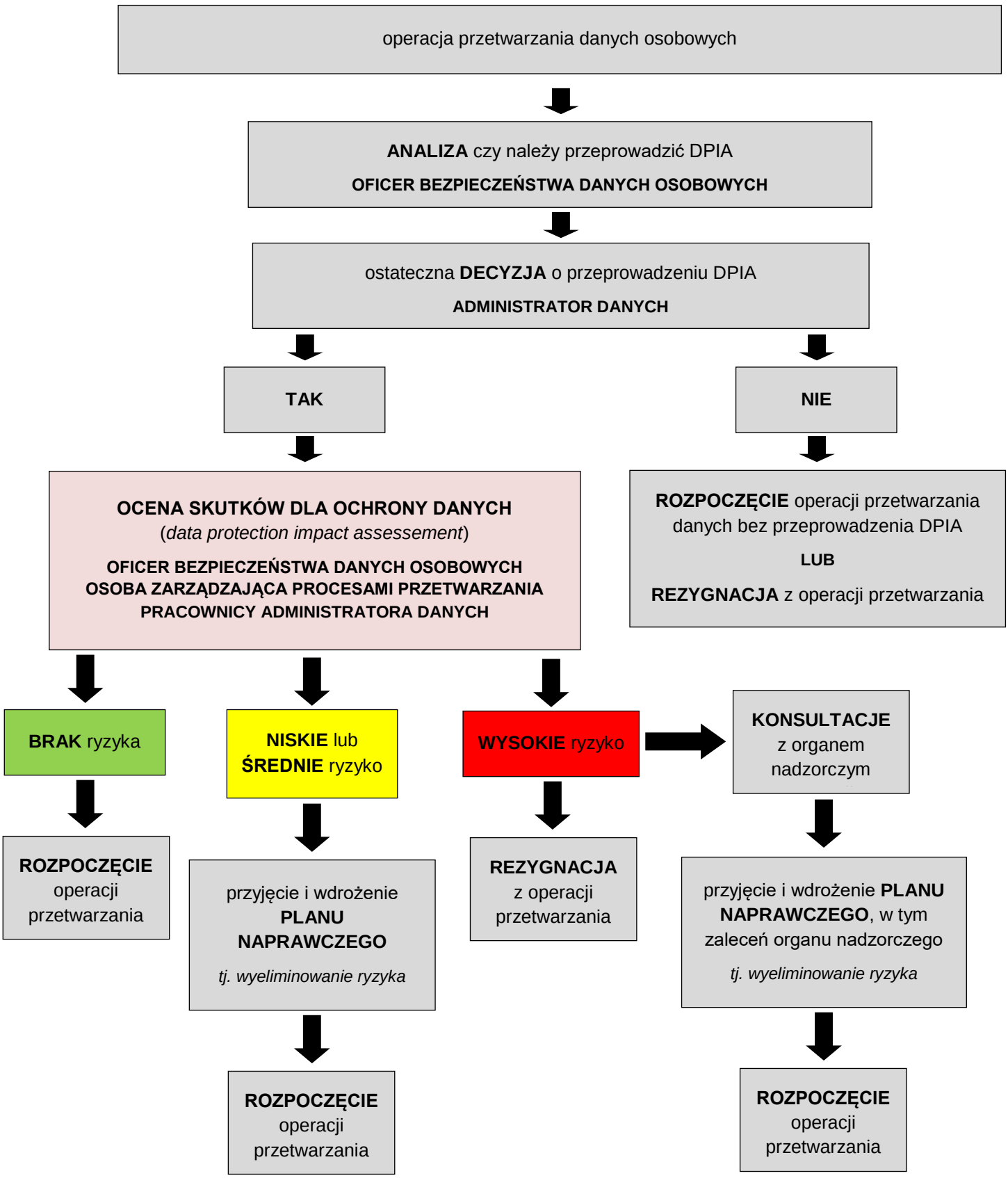
26.4. dane kontaktowe OBDO,

26.5. ocenę skutków dla ochrony danych, o której mowa w pkt 21,

26.6. wszelkie inne informacje, których żąda organ nadzorczy.

24. OBDO wspiera Administratora Danych w konsultacjach z organem nadzorczym, o których mowa w pkt 26 i 27 powyżej, w szczególności, przy współudziale Osoby zarządzającej procesami przetwarzania danych osobowych, kompletuje oraz przygotowuje wymagane dokumenty i oświadczenia.

Schemat graficzny procedury



ANALIZA **CZY OPERACJA PRZETWARZANIA DANYCH OSOBOWYCH BĘDZIE PODLEGAŁA OBOWIĄZKOWI PRZEPROWADZENIA DPIA**			
***Wypełnia Oficer Bezpieczeństwa Danych Osobowych**			
1.	**Administrator Danych**		
2.	**Imię i nazwisko Oficera Bezpieczeństwa Danych Osobowych**		
3.	**Data analizy** **dd/mm/rrrr*		
4.	**Operacja przetwarzania danych osobowych poddawana analizie** **Należy jednoznacznie wskazać operację przetwarzania danych osobowych poddawaną analizie, w szczególności poprzez dokonanie opisu operacji, czy też odwołanie do Rejestru czynności przetwarzania*		
5.	**Analiza** **Należy wskazać, które ze wskazanych kryteriów spełnia operacja przetwarzania poddawana analizie*	**Dany rodzaj przetwarzania został wskazany w wykazie ustanowionym przez organ nadzorczy jako podlegający wymogowi dokonana oceny skutków dla ochrony danych osobowych**	☐ tak ☐ nie Uwagi: …
		Ocena lub punktacja ***Operacja obejmuje dokonywanie oceny lub punktacji w tym profilowanie i prognozowanie, w szczególności na podstawie aspektów dotyczących efektów pracy, sytuacji ekonomicznej,**	☐ tak ☐ nie Uwagi: …

		zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą	
		Zautomatyzowane podejmowanie decyzji o skutku prawnym lub podobnie znaczącym skutku ***Operacja obejmuje przetwarzanie mające na celu podjęcie decyzji w sprawie osób, których dane dotyczą, wywołujących skutki prawne wobec osoby fizycznej lub decyzji, które w podobny sposób istotnie na nią wpływają*	☐ tak ☐ nie Uwagi: …
		Systematyczne monitorowanie ***Operacja obejmuje przetwarzanie wykorzystywane do obserwacji, monitorowania lub kontrolowania osób, których dane dotyczą, w tym danych gromadzonych za pośrednictwem sieci lub w ramach systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie*	☐ tak ☐ nie Uwagi: …
		Szczególne kategorie danych lub dane osobowe podlegające szczególnym warunkom przetwarzania **Operacja obejmuje przetwarzanie szczególnych kategorii danych osobowych określonych w art. 9 RODO i / lub dane osobowe dotyczące wyroków skazujących za przestępstwo lub czynów zabronionych zdefiniowane w art. 10 RODO*	☐ tak ☐ nie Uwagi: …
		Przetwarzanie na dużą skalę **Operacja obejmuje przetwarzanie danych na dużą skalę, przy uwzględnieniu w szczególności takich czynników jak: liczba osób, których dane dotyczą, ilość danych lub zakres poszczególnych przetwarzanych pozycji danych, czas trwania lub trwałość czynności przetwarzania danych, zakres geograficzny czynności przetwarzania*	☐ tak ☐ nie Uwagi: …
		Dopasowywanie lub łączenie zbiorów danych	☐ tak

		**Operacja obejmuje dopasowywanie lub łączenie zbiorów danych np. danych pochodzących z co najmniej dwóch operacji przetwarzania przeprowadzonych w różnych celach lub przez różnych administratorów w sposób wykraczający poza uzasadnione oczekiwania osób, których dane dotyczą*	☐ nie Uwagi: …
		Dane dotyczące osób wymagających szczególnej opieki **Operacja obejmuje przetwarzanie danych osób wymagających szczególnej opieki, w szczególności przetwarzanie danych dzieci, pracowników, bardziej wrażliwych grup społecznych wymagające szczególnej ochrony (osoby chore psychicznie, osoby starsze, itp.) i / lub można stwierdzić brak równowagi między stanowiskiem osoby, której dane dotyczą, a stanowiskiem Administratora Danych*	☐ tak ☐ nie Uwagi: …
		Innowacyjne wykorzystanie lub stosowanie nowych rozwiązań technologicznych lub organizacyjnych **Operacja obejmuje innowacyjne wykorzystanie lub stosowanie nowych rozwiązań technologicznych lub organizacyjnych, w szczególności takich jak połączenie technologii rozpoznającej odcisk palca i twarz w celu poprawy fizycznej kontroli dostępu itd.*	☐ tak ☐ nie Uwagi: …
		Przetwarzanie uniemożliwia osobom, których dane dotyczą, wykonywanie prawa lub korzystanie z usługi lub umowy **Operacja obejmuje przetwarzanie, którego skutkiem może być uniemożliwienie osobom, których dane dotyczą, wykonywania przysługujących im praw lub korzystania z usługi lub umowy*	☐ tak ☐ nie Uwagi: …
6.	**Kwalifikacja operacji przetwarzania** **Należy wskazać, czy operacja przetwarzania danych będzie podlegała obowiązkowi przeprowadzenia DPIA*	Operacja przetwarzania danych osobowych ☐ **podlega** ☐ **nie podlega**	

		obowiązkowi przeprowadzenia oceny skutków dla ochrony danych osobowych (*data protection impact assessment)*
7.	**Uzasadnienie** **Należy przedstawić krótkie uzasadnienie do dokonanej klasyfikacji operacji przetwarzania danych*	

PAPORT Z OCENY SKUTKÓW DLA OCHRONY DANYCH OSOBOWYCH (DATA PROTECTION IMPACT ASSESSEMENT)

……

miejscowość, data

1. Administrator Danych: ……..

2. Oficer Bezpieczeństwa Danych Osobowych ……..…….…….

3. Osoby uczestniczące w ocenie skutków dla ochrony danych osobowych:

   3.1. ……

   3.2. ……....

   3.3. ……

   3.4. ……

4. Data rozpoczęcia oceny skutków dla ochrony danych osobowych: ……..……..…

5. Data zakończenia oceny skutków dla ochrony danych osobowych: ……..…….

6. Operacja przetwarzania danych osobowych podlegająca ocenie skutków dla ochrony danych osobowych:

   **systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez Administratora Danych*

   ……

   ……

   ……

   ……

7. Opinia osób, których dane dotyczą lub ich przedstawicieli:

   ☐ nie dotyczy

☐ tak

Opis:

……

……

……

……

8. Ocena skutków dla ochrony danych osobowych:

Ocena niezbędności i proporcjonalności operacji:

**ocena czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów*

……

……

……

……

Stwierdzony poziom ryzyka dla operacji:

**ocena ryzyka naruszenia praw lub wolności osób, których dane dotyczą*

☐ brak

☐ niski

☐ średni

☐ wysoki

Uzasadnienie:

……

……

……

……

9. Plan naprawczy:

Proponowane środki, które powinny zostać podjęte w celu zaradzenia ryzyku bądź jego zminimalizowaniu:

**środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie Ogólnego rozporządzenia o ochronie danych, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy*

……

……

……

……

10. Organ nadzorczy:

Konsultacja z organem nadzorczym:

☐ wymagana

☐ niewymagana

Uzasadnienie:

……

……

……

……

11. Załączniki:

1) Karta oceny skutków dla ochrony danych Filar I LEGALNOŚĆ;

2) Karta oceny skutków dla ochrony danych Filar II ŚWIADOMOŚĆ;

3) Karta oceny skutków dla ochrony danych Filar III ZABEZPIECZENIA;

4) Karta oceny skutków dla ochrony danych Filar IV OBOWIĄZKI WZGLĘDEM REGULATORA;

5) Karta oceny skutków dla ochrony danych Filar V PRAWA OSÓB, KTÓRYCH DANE DOTYCZĄ;

6) Matryca oceny skutków dla ochrony danych.

……

Data i podpis

Oficera Bezpieczeństwa Danych Osobowych

Otrzymują:

1 x oryginał Administrator Danych

1 x kopia Oficer Bezpieczeństwa Danych Osobowych

ANALIZA preDPIA oraz OGÓLNA OCENA POZIOMU RYZYKA PROCESU		Wskazówki metodologiczne
Administrator danych **nazwa, siedziba*		*należy zidentyfikować Administratora danych*
Proces przetwarzania danych osobowych		*należy jednoznacznie wskazać proces przetwarzania danych osobowych poddawaną analizie, w szczególności poprzez dokonanie opisu procesu, czy też odwołanie do Rejestru czynności przetwarzania*
Osoby biorące udział w analizie		*należy wskazać imiona, nazwiska oraz stanowiska osób biorących udział w analizie (pracowników / współpracowników administratora danych), tj. udzielających informacji na wskazane w analizie zagadnienia oraz wskazać ich role w zakresie przeprowadzanej analizy*

**pola oznaczone na ŻÓŁTO wypełnia Lex Artist*

ZAGADNIENIE		ODPOWIEDŹ	UZASADNIENIE *pola oznaczone jako n/a nie wymagają uzasadnienia*	WSKAZÓWKI METODOLOGICZNE	ANALIZA preDPIA	OGÓLNA OCENA POZIOMU RYZYKA
Wykaz ustanowiony przez organ nadzorczy		TAK	n/a	*należy określić, czy dany proces przetwarzania został wskazany w wykazie ustanowionym przez Prezesa Urzędu Ochrony Danych Osobowych jako podlegający wymogowi dokonania oceny skutków dla ochrony danych osobowych aktualny wykaz dostępny jest pod linkiem: https://monitorpolski.gov.pl/MP/2019/666*	1	1
Ocena lub punktacja		TAK	*jeżeli TAK - jaką ocenę lub punktację się stosuje?*	*należy określić, czy proces obejmuje dokonywanie oceny lub punktacji, w tym profilowanie i prognozowanie, w szczególności na podstawie aspektów dotyczących efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą*	1	1
Zautomatyzowane podejmowanie decyzji o skutku prawnym lub podobnie znaczącym skutku		TAK	*jeżeli TAK - na czym polega dokonywane zautomatyzowane podejmowanie decyzji o skutku prawnym lub podobnie znaczącym skutku*	*należy określić, czy proces obejmuje przetwarzanie mające na celu podjęcie decyzji w sprawie osób, których dane dotyczą, wywołujących skutki prawne wobec osoby fizycznej lub decyzji, które w podobny sposób istotnie na nią wpływają, przykładowo przetwarzanie może prowadzić do wykluczenia lub dyskryminacji osób fizycznych*	1	1
Systematyczne monitorowanie			*jeżeli TAK - na czym polega systematyczne monitorowanie?*	*należy określić, czy proces obejmuje przetwarzanie wykorzystywane do obserwacji, monitorowania lub kontrolowania osób, których dane dotyczą, w tym danych gromadzonych za pośrednictwem sieci lub w ramach systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie*	0	0
Szczególne kategorie danych lub dane osobowe podlegające szczególnym warunkom przetwarzania	**pochodzenie rasowe lub etniczne**	TAK	n/a	*należy określić, czy w ramach procesu przetwarza się informacje ujawniające pochodzenie rasowe lub etniczne osoby, której dane dotyczą*	1	5
	poglądy polityczne	TAK	n/a	*należy określić, czy w ramach procesu przetwarza się informacje ujawniające poglądy polityczne osoby, której dane dotyczą*		5
	przekonania religijne lub światopoglądowe	TAK	n/a	*należy określić, czy w ramach procesu przetwarza się informacje ujawniające przekonania religijne lub światopoglądowe osoby, której dane dotyczą (np. informacje o wyznaniu)*		5
	przynależność do związków zawodowych	TAK	n/a	*należy określić, czy w ramach procesu przetwarza się informacje ujawniające przynależność do związków osoby, której dane dotyczą*		5
	dane genetyczne	TAK	n/a	*należy określić, czy w ramach procesu przetwarza się informacje ujawniające dane genetyczne osoby, której dane dotyczą*		5
	dane biometryczne	TAK	n/a	*należy określić, czy w ramach procesu przetwarza się informacje ujawniające dane biometryczne osoby, której dane dotyczą pozwalające na jednoznaczne zidentyfikowanie tej osoby (np. skan tęczówki oka / odcisk palca przetwarzany w ramach systemu kontroli dostępu do pomieszczeń / systemów informatycznych)*		5
	dane dotyczące zdrowia	TAK	n/a	*należy określić, czy w ramach procesu przetwarza się informacje ujawniające stan zdrowia osoby, której dane dotyczą*		5
	dane dotyczące seksualności lub orientacji seksualnej	TAK	n/a	*należy określić, czy w ramach procesu przetwarza się informacje ujawniające seksualność lub orientację seksualną osoby, której dane dotyczą*		5
	dane dotyczące wyroków skazujących	TAK	n/a	*należy określić, czy w ramach procesu przetwarza się informacje dotyczące wyroków skazujących tj. wyroków karnych (w sprawach o wykroczenia / przestępstwa)*		5
	dane dotyczące czynów zabronionych	TAK	n/a	*należy określić, czy w ramach procesu przetwarza się informacje o popełnionych wykroczeniach / przestępstwach (np. oświadczenia o niekaralności)*		5
Przetwarzanie na dużą skalę	**liczba osób, których dane dotyczą**	10000	*należy wyjaśnić, w jaki sposób określono podaną liczbę*	*należy określić szacunkową liczbę osób, których dane osobowe są przetwarzane w procesie, co do zasady należy przyjąć liczbę osób, których dane dotyczą przypadającą na dzień dokonywania analizy, w przypadku procesów, które nie są prowadzone w sposób bieżący (np. rekrutacja) należy uwzględnić średnią liczbę osób, których dane przetwarzane są*	0	7
	łączna liczba kategorii przetwarzanych danych	1000000	*należy wyjaśnić, w jaki sposób określono podaną liczbę*	*należy określić szacunkową liczbę kategorii danych osobowych przetwarzanych w procesie (liczba osób x liczba kategorii danych osobowych)* *np. w bazie newsletter przetwarza się imię oraz email subskrybenta, baza liczy 10 subskrybentów, oznacza to, że liczba osób, których dane dotyczą wynosi 10, natomiast liczba kategorii danych wynosi 20 (dla każdego subskrybenta przetwarzane są*		20
	czas trwania przetwarzania	5	n/a	*należy określić szacunkowy czas trwania przetwarzania, na podstawie stosowanych zasad retencji (ujawnionych w rejestrze czynności przetwarzania lub innej dokumentacji ochrony danych osobowych (np. Polityce ochrony danych osobowych)) wartość należy podać w latach* *np. dane osobowe pracowników przetwarza się przez okres 50 lat od zakończenia stosunku pracy, a w przypadku nieprowadzenia*		2
	zakres geograficzny	Polska oraz poza Polską	*jeżeli poza Polską - jakie państwo / państwa?*	*należy określić zakres geograficzny przetwarzania danych osobowych*		2
	duża skala przetwarzania	NIE	*jeżeli TAK - jak uzasadnia się przyjęcie dużej skali przetwarzania?*	*na podstawie informacji ujawnionych w wierszach 23-27 należy dokonać oceny skali przetwarzania danych osobowych w procesie*		
Dopasowywanie lub łączenie zbiorów danych			*jeżeli TAK - na czym polega dopasowywanie lub łączenie zbiorów danych?*	*należy określić, czy proces obejmuje dopasowywanie lub łączenie zbiorów danych np. danych pochodzących z co najmniej dwóch procesów przetwarzania przeprowadzonych w różnych celach lub przez różnych administratorów w sposób wykraczający poza uzasadnione oczekiwania osób, których dane dotyczą*	0	0
Dane dotyczące osób wymagających szczególnej opieki	**osoby starsze (powyżej 60 r.ż.)**		n/a	*należy określić, czy proces ze swojego założenia obejmuje przetwarzanie danych osób wymagających szczególnej opieki, tj. osób starszych* *np. usługa kierowana bezpośrednio do osób starszych (ubezpieczenie dla osób pow. 60 r.ż.)*	0	0
	dzieci (poniżej 13 r.ż.)		n/a	*należy określić, czy proces ze swojego założenia obejmuje przetwarzanie danych osób wymagających szczególnej opieki, tj. dzieci* *np. usługa kierowana bezpośrednio do dzieci (platforma internetowa z grami)*	0	0
	osoby niepełnosprawne		n/a	*należy określić, czy proces ze swojego założenia obejmuje przetwarzanie danych osób wymagających szczególnej opieki, tj. osób niepełnosprawnych* *np. usługa kierowana bezpośrednio do osób niepełnosprawnych (aplikacja dla osób niewidomych)*	0	0
Innowacyjne wykorzystanie lub stosowanie nowych rozwiązań technologicznych lub organizacyjnych			*jeżeli TAK - na czym polega to innowacyjne wykorzystanie lub stosowanie nowych rozwiązań technologicznych lub organizacyjnych?*	*należy określić, czy proces obejmuje innowacyjne wykorzystanie lub stosowanie nowych rozwiązań technologicznych lub organizacyjnych* *np. połączenie technologii rozpoznającej odcisk palca i twarz w celu poprawy fizycznej kontroli dostępu*	0	0
Przetwarzanie uniemożliwia osobom, których dane dotyczą, wykonywanie prawa lub korzystanie z usługi lub umowy			*jeżeli TAK - jakie prawa / usługi / umowy nie mogą być realizowane?*	*należy określić, czy proces obejmuje przetwarzanie, którego skutkiem może być uniemożliwienie osobom, których dane dotyczą, wykonywania przysługujących im praw lub korzystania z usługi lub umowy* *np. monitoring wizyjny przy wejściu do sklepu / hotelu, gdzie bez wkroczenia w obszar monitorowany (przetwarzanie danych*	0	0
Liczba osób mających dostęp do przetwarzanych danych		60	n/a	*należy wskazać liczbę osób, które mają dostęp do danych osobowych przetwarzanych w ramach procesu* *dotyczy wyłącznie osób wchodzących w skład wewnętrznej struktury organizacyjnej (pracownicy / współpracownicy), nie dotyczy pracowników / współpracowników podmiotów zewnętrznych*		2
Liczba systemów IT, w których przetwarzane są dane osobowe		5	*należy wskazać nazwy systemów* *1) nazwa systemu* *2) nazwa systemu*	*należy wskazać liczbę systemów informatycznych w ramach, których dochodzi do przetwarzania danych osobowych w procesie*		3
Liczba nadanych dostępów do systemów IT, w których przetwarzane są dane osobowe		1000	*należy wskazać ilość przyznanych dostępów w odniesieniu do poszczególnych systemów:* *1) system 1 - ilość dostępów x* *2) system 2 - ilość dostępów x*	*należy wskazać liczbę dostępów nadanych do systemów informatycznych w ramach, których dochodzi do przetwarzania danych osobowych w procesie poddawanym analizie*		15
Liczba podmiotów, którym powierza się przetwarzanie danych osobowych			*należy podać nazwy podmiotów*	*należy wskazać liczbę podmiotów, którym powierza się dane osobowe przetwarzane w ramach procesu poddawanej analizie*		0
Dane finansowe			n/a	*należy wskazać, czy w zakresie danych osobowych przetwarzanych w ramach procesu znajdują się informacje o charakterze finansowym (w szczególności dane dotyczące wynagrodzenia za pracę / usługi, informacje o przyznanych świadczeniach socjalnych (np. w ramach ZFŚS), etc.)*		0
Dane płatnicze			n/a	*należy wskazać, czy w zakresie danych osobowych przetwarzanych w ramach procesu znajdują się informacje dotyczące kart płatniczych (kredytowch / debetowych / etc.) takie jak np. numery kart, kody bezpieczeństwa, rodzaj karty, etc.* **dotyczy tylko i wyłącznie przypadków zbierania danych dla własnych celów*		0
Państwo trzecie (poza EOG)		TAK, (co najmniej jedno) państwo bez decyzji Komisji Europejskiej	*należy wskazać nazwę państwa*	*należy wskazać czy dane osobowe są transferowane do państwa trzeciego (tj. państwa poza Europejskim Obszarem Gospodarczym)*		5

PESEL		n/a	należy wskazać, czy w zakresie danych osobowych przetwarzanych w ramach procesu znajduje się PESEL	0
Forma przetwarzania danych		n/a	należy wskazać formę przetwarzania danych osobowych w procesie	0

OCENA KOŃCOWA ANALIZY

**ocena końcowa formułowana jest na podstawie wskazanych powyżej informacji, otrzymanych od osób biorących udział w analizie (pracowników / współpracowników administratora danych)*

** wypełnia Lex Artist*

DPIA *(data protection impact assessement)*		**TAK**	**Uzasadnienie** [uzasadnienie analizy]
Ogólna ocena poziomu ryzyka	**Liczba uzyskanych punktów ryzyka**	**109**	**Uzasadnienie** [uzasadnienie analizy]
	Procent uzyskanych punktów ryzyka	**66%**	
	Poziom ryzyka 0 - 10 % Poziom niski 11 - 35 % Poziom średni 36 - 55 % Poziom wysoki <55% Poziom bardzo wysoki	**Poziom bardzo wysoki**	

Załącznik nr 8 – Procedura testu równowagi prawnie uzasadnionego interesu Administratora Danych (*balancing test)*

1. Test równowagi polega na porównaniu prawnie uzasadnionych interesów realizowanych przez Administratora Danych w związku z konkretnymi czynnościami przetwarzania danych osobowych z interesami lub podstawowymi prawami i wolnościami osoby, której dane dotyczą.
2. OBDO informuje Administratora Danych o konieczności przeprowadzenia testu równowagi dla konkretnego procesu przetwarzania danych osobowych. Administrator Danych podejmuje ostateczną decyzję w zakresie rozpoczęcia realizacji testu równowagi.
3. Test równowagi przeprowadzany jest przez OBDO, przy współpracy z:
   3.1. Osobą zarządzającą procesami przetwarzania danych osobowych,
   3.2. ASI,
   3.3. pracownikami Administratora Danych uczestniczącymi w procesie przetwarzania danych osobowych, który podlega testowi równowagi.
4. Test równowagi składa się z następujących etapów:
   4.1. zidentyfikowanie prawnie uzasadnionych interesów Administratora Danych lub strony trzeciej, realizowanych w związku z przetwarzaniem danych osobowych w określonym celu,
   4.2. zidentyfikowanie interesów lub podstawowych praw i wolności osoby, której dane dotyczą, a które mogą być naruszone przez przetwarzanie danych osobowych,
   4.3. ustalenie, czy przetwarzanie danych osobowych w danych okolicznościach jest konieczne do zrealizowania prawnie uzasadnionego interesu Administratora Danych lub strony trzeciej,
   4.4. dokonanie ważenia interesów Administratora Danych lub strony trzeciej i osoby, której dane dotyczą.
5. Ważenie interesów podczas przeprowadzanego testu równowagi, polega na określeniu, czyje interesy mają charakter nadrzędny. Podczas ważenia interesów uwzględnia się, w szczególności:
   5.1. charakter danych osobowych,
   5.2. kategorie osób, których dane dotyczą,
   5.3. relacje zachodzące pomiędzy Administratorem Danych, a osobą, której dane dotyczą,
   5.4. uzasadnione oczekiwania osób, których dane dotyczą,
   5.5. sposób przetwarzania danych,
   5.6. ewentualne szkody Administratora Danych związane z zaniechaniem przetwarzania,
   5.7. zastosowane środki bezpieczeństwa.
6. OBDO wykonuje test równowagi zgodnie ze wzorem wskazanym w niniejszym Załączniku, tj. poprzez uzupełnienie:

6.1. wzoru *Testu równowagi prawnie uzasadnionych interesów Administratora Danych* - obligatoryjnie,

6.2. wzoru *Załącznika do Testu równowagi prawnie uzasadnionego interesu Administratora Danych* – fakultatywnie, tj. wyłącznie wówczas, gdy OBDO uzna, że z uwagi na charakter i sposób przetwarzania danych osobowych w analizowanym procesie, zachodzi potrzeba dodatkowego przeanalizowania stosowanych zabezpieczeń ochrony danych.

7. OBDO dokumentuje przeprowadzaną przez siebie analizę oraz wynik testu równowagi.

8. Wynik testu równowagi może być:

8.1. pozytywny dla Administratora Danych tj. interesy osoby, której dane dotyczą nie są nadrzędne wobec interesów Administratora Danych lub strony trzeciej,

8.2. negatywny dla Administratora Danych tj. interesy osoby, której dane dotyczą są nadrzędne wobec interesów Administratora Danych lub strony trzeciej.

9. Wynik testu równowagi jest negatywny dla Administratora Danych w szczególności wówczas, gdy istnieje możliwość zrealizowania tego samego celu bez konieczności przetwarzania danych osobowych lub ograniczając ich przetwarzanie.

10. OBDO przekazuje Administratorowi Danych, wynik testu równowagi.

11. Jeżeli wynik testu równowagi jest negatywny dla Administratora Danych, wraz z tym wynikiem OBDO przekazuje Administratorowi Danych rekomendacje w zakresie dalszego przetwarzania danych osobowych. Rekomendacje mogą dotyczyć, w szczególności:

11.1. wdrożenia odpowiednich środków naprawczych mających wpływ na wzajemne interesy Administratora Danych lub stron trzecich i osoby, której dane dotyczą,

11.2. zmiany podstawy prawnej przetwarzania danych osobowych w procesie,

11.3. zaprzestania przetwarzania danych osobowych w procesie.

12. Na podstawie przedstawionego wyniku testu równowagi Administrator Danych podejmuje decyzję odnośnie do dalszego przetwarzania danych osobowych w procesie.

13. Jeżeli wynik testu równowagi jest negatywny dla Administratora Danych i podjął on decyzję o wdrożeniu rekomendowanych przez OBDO odpowiednich środków naprawczych, wówczas za koordynację ich wdrożenia odpowiada OBDO.

14. Po wdrożeniu środków, o których mowa w pkt 13, OBDO ponownie przeprowadza test równowagi na zasadach opisanych w niniejszym Załączniku.

15. W przypadkach, kiedy już po przeprowadzeniu testu równowagi, proces przetwarzania uległ znaczącej zmianie w stosunku do jego pierwotnego charakteru i może mieć wpływ na wzajemne interesy Administratora Danych lub strony trzeciej i osoby, której dane dotyczą, test równowagi powinien zostać wykonany ponownie, na zasadach opisanych w niniejszym Załączniku.

TEST RÓWNOWAGI PRAWNIE UZASADNIONEGO INTERESU ADMINISTRATORA DANYCH		
1.	**Administrator Danych**	
2.	**Imię i nazwisko osoby wykonującej test** *OBDO lub inna osoba działająca w imieniu Administratora Danych*	
3.	**Ogólny opis operacji przetwarzania** *Należy opisać proces biznesowy w ramach którego będzie dochodziło do przetwarzania danych*	
Spojrzenie na proces przetwarzania z perspektywy Administratora Danych lub strony trzeciej		
4.	**Czy i jaki jest interes jest realizowany przez Administratora Danych lub stronę trzecią? Czy przetwarzanie jest realizowane w ramach interesu społecznego?** *Należy w sposób konkretny opisać na czym polega interes Administratora Danych lub strony trzeciej, przy założeniu, że interes taki musi mieć znaczenie gospodarcze oraz musi być:* *- zgodny prawem (prawem UE i krajowym),* *- jasno i konkretnie wyrażony,* *-być interesem rzeczywistym, (a nie opartym na przypuszczeniach),* *- zgodny z przedmiotem działalności Administratora Danych.* *Interes społeczny występuje wtedy, gdy korzyść z przetwarzania może osiągnąć także społeczeństwo lub określone grupy społeczeństwa.*	☐ tak *(należy wskazać jaki)*: … ☐ nie
5.	**Jakie korzyści wynikają z przetwarzania danych? Jakie ewentualne szkody mogą wyniknąć, jeżeli przetwarzanie danych nie będzie miało miejsca?**	

	Należy ocenić korzyści wynikające z przetwarzania danych dla Administratora Danych lub strony trzeciej (lub społeczność) oraz ewentualne szkody poniesione przez nich, jeżeli przetwarzanie danych nie będzie miało miejsca.	
6.	**Czy przetwarzanie danych jest niezbędne?** *Należy ustalić czy przetwarzanie danych osobowych jest faktycznie niezbędne dla osiągnięcia celu Administratora Danych, czy też istnieje inna, mniej ingerująca w prywatność metoda zapewniająca osiągnięcie interesu.* *Niezbędność zachodzi także wtedy, gdy osiągniecie zakładanego interesu bez przetwarzania danych wiązałoby się z niewspółmiernym wysiłkiem, czasem lub kosztami.*	☐ tak (*należy określić na czym polega*): … ☐ nie
Spojrzenie na proces przetwarzania z perspektywy osoby, której dane dotyczą		
7.	**Jakie prawa i wolności / interesy występują po stronie osoby, której dane dotyczą?** *Należy opisać jaki jest interes po stronie osoby, który wymaga ochrony danych osobowych lub jakie są prawa i wolności po stronie osoby, które wymagają ochrony.* *Takimi prawami będą w szczególności prawa zagwarantowane w Karcie Praw Podstawowych UE, Europejskiej Konwencji Praw Człowieka, Konstytucji.*	
8.	**Jaka relacja zachodzi między Administratorem Danych, a osobą, której dane dotyczą?** *Należy określić, jaka relacja łączy Administratora Danych z osobą, której dane dotyczą, w szczególności może to nastąpić poprzez określenie kategorii osób, których dane są przetwarzane (kandydat do pracy, który wysłał swoje dokumenty aplikacyjne, pracownik, współpracownik, osoba, która wyraziła zgodę na otrzymywanie informacji handlowych, klient z aktywną umową, uśpiony klient, etc.).* *Jeśli wskazano więcej niż jedną kategorię osób, których dane dotyczą, należy w przybliżeniu procentowo oszacować udział każdej z kategorii.*	☐ tak (*określić jaka relacja*): … ☐ brak relacji

9.	**Czy osoba, której dane dotyczą spodziewa się, że jej dane będą przetwarzane w tym celu?** *Należy ocenić czy w świetle rozsądnych oczekiwań osoba może się spodziewać przetwarzania jej danych.*	☐ tak *(opis z czego to wynika):* … ☐ nie
10.	**Czy osoba, której dane dotyczą ma kontrolę nad przetwarzanymi danymi?** *Należy określić w jaki sposób osoba jest informowana o swoich prawach oraz w jaki następuje realizacja każdego ze wskazanych praw.*	☐ tak *(należy wskazać poniżej):* - prawo dostępu do danych: … - prawo do sprostowania: … - prawo do usunięcia: … - prawo do ograniczenia przetwarzania: … - prawo do sprzeciwu: … ☐ nie *(powód braku kontroli): …*
11.	**Czy przetwarzane dane będą dotyczyły osób wymagających szczególnej opieki?**	☐ dzieci (*należy określić wiek*): … ☐ osoby starsze ☐ osoby niepełnosprawne ☐ inne (*należy określić jakie*): … ☐ nie

<table>
<tr><td rowspan="2">12.</td><td rowspan="2">Jaki rodzaj danych osobowych będzie przetwarzany?

Należy wskazać jakie kategorie danych będą przetwarzane, tj.: „dane zwykłe”, szczególne kategorie danych (art. 9 RODO) lub dane osobowe dotyczące wyroków skazujących i czynów zabronionych (art. 10 RODO).</td><td rowspan="2">Dane zwykłe:

☐ imię

☐ nazwisko

☐ adres zamieszkania

☐ adres prowadzenia działalności gospodarczej

☐ adres email

☐ data urodzenia

☐ PESEL

☐ NIP

☐ inne (należy określić jakie): …</td><td>Szczególne kategorie danych:

☐ pochodzenie rasowe lub etniczne

☐ poglądy polityczne

☐ przekonania religijne lub światopoglądowe

☐ przynależność do związków zawodowych

☐ dane genetyczne

☐ dane biometryczne

☐ dane dotyczące zdrowia

☐ seksualność lub orientacja seksualna</td></tr>
<tr><td>Dane osobowe dotyczą:

☐ wyroków skazujących

☐ czynów zabronionych lub powiązanych środków bezpieczeństwa</td></tr>
<tr><td colspan="4">Organizacja przetwarzania danych osobowych</td></tr>
<tr><td rowspan="3">13.</td><td rowspan="3">Jak duża jest planowana skala przetwarzania?

Należy określić jaka jest skala przetwarzania danych.</td><td colspan="2">Szacowana liczba osób, których dane dotyczą: …</td></tr>
<tr><td colspan="2">Szacowana liczba rekordów przetwarzanych danych: …</td></tr>
<tr><td colspan="2">Szacowana ilość osób mających dostęp do przetwarzanych danych: …</td></tr>
<tr><td>14.</td><td>W jaki sposób dane będą przetwarzane?

Należy wskazać czy dane będą przetwarzane w sposób zautomatyzowany i wykorzystywane do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej</td><td colspan="2">Profilowanie:

☐ tak (należy opisać w jaki sposób)

☐ nie</td></tr>
</table>

	osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się. *** Należy wskazać czy w ramach przetwarzania danych będzie dochodziło do podejmowania decyzji, opierających się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołujących wobec osoby, której dane dotyczą skutki prawne lub w podobny sposób istotnie na nią wpływających.* *** Należy wskazać czy w ramach planowanej operacji przetwarzania wykorzystywane będą innowacyjne rozwiązania technologiczne lub organizacyjne (np. takie jak połączenie technologii rozpoznającej odcisk palca i twarz w celu poprawy fizycznej kontroli dostępu, obserwacja, monitorowanie lub kontrolowanie osób, których dane dotyczą, etc.).* **** Dot. np. przypadku zamieszczania danych na ogólnodostępnych stronach www.*	Zautomatyzowane podejmowanie decyzji**: ☐ tak *(należy opisać w jaki sposób)* ☐ nie
		Innowacyjne rozwiązania technologiczne lub organizacyjne***: ☐ tak (*należy wskazać jakich*): … ☐ nie
		Ujawnianie wielu osobom lub publikacja****: ☐ tak (*należy wskazać jaki sposób*): … ☐ nie
15.	**Czy w przetwarzaniu danych będą brały udział inne podmioty?** *Należy wskazać czy dane osobowe będą (mogą być) przekazywane innym podmiotom, a jeżeli tak, to jakie to będą kategorie podmiotów i cel przekazania.* *Należy wskazać, czy będzie dochodziło do współadministrowania danymi osobowymi w rozumieniu art. 26 RODO*	Przekazywanie danych: ☐ w ramach grupy Administratora Danych *(należy określić kategorie odbiorców oraz cel)*: … ☐ podmiotom upoważnionym do otrzymania danych na podstawie przepisów prawa *(należy określić kategorie odbiorców oraz cel): …* ☐ innym podmiotom zewnętrznym (w ramach EOG) *(należy określić kategorie odbiorców oraz cel): …* ☐ innym podmiotom zewnętrznym (poza EOG) *(należy określić kategorie odbiorców oraz cel): …*
		Współadministrowanie: ☐ tak ☐ nie
16.	**Czy i w jaki sposób określono okresy retencyjne?** *Należy określić szacunkowy czas przetwarzania danych osobowych.*	Szacowany czas przetwarzania danych wynosi: …

17.	**Jakie będą stosowane środki zabezpieczeń organizacyjnych, fizycznych i technicznych?** *Należy określić konkretne środki zabezpieczeń stosowane w odniesieniu do przetwarzania danych w procesie którego dotyczy Test, np.: wdrożenie określonych Polityk Ochrony Danych, szkolenia pracowników, szyfrowanie danych, itp.* *W przypadku gdy istnieje już dokument opisujący stosowane środki zabezpieczeń, należy powołać się na ten dokument podając jego pełną nazwę oraz (gdy to możliwe) datę wdrożenia* **Zalecane w odniesieniu do:* *- złożonych procesów przetwarzania danych, w tym takich w których stosowane są zaawanasowane rozwiązania technologiczne lub organizacyjne (np. pkt. 14 powyżej),* *- procesów w których przetwarzane są dane na dużą skalę,* *-procesów w których przetwarzane są szczególe kategorie danych lub dane dotyczące wyroków skazujących i czynów zabronionych.*	Środki zabezpieczeń organizacyjnych ☐ tak (*należy wskazać jakie, w tym poprzez odwołanie się do określonych procedur*): … ☐ brak
		Środki zabezpieczeń technicznych ☐ tak (*należy wskazać jakie, w tym poprzez odwołanie się do określonych procedur*): … ☐ brak
		Środki zabezpieczeń fizycznych ☐ tak (*należy wskazać jakie, w tym poprzez odwołanie się do określonych procedur*): … ☐ brak
		(*opcjonalnie*) Załącznik nr 1 – *Opis stosowanych zabezpieczeń** ☐ tak ☐ nie (*brak potrzeby*)
18.	**Czy zastosowano dodatkowe środki ochronne?** *W oparciu o wytyczne z Opinii Grupy Roboczej art. 29 ds. Ochrony Danych nr. 6/2014 z dnia 9 kwietnia 2014 r. w sprawie pojęcia prawnie uzasadnionych interesów administratora danych na mocy artykułu 7 dyrektywy 95/46*	☐ minimalizacja danych (*wskazać w jaki sposób np. poprzez ograniczenie ilości zbieranych danych do minimum, natychmiastowe usunięcie danych po ich wykorzystaniu)*: … ☐ łatwo dostępny mechanizm *opt-out* ☐ bezpośredni dostęp do danych (za pośrednictwem udostępnionych narzędzi IT) ☐ zwiększona przejrzystość przetwarzania np. poprzez stosowanie symboli graficznych ☐ oddzielenie funkcjonalne danych
	Podsumowanie	
19.	**Czy interes lub podstawowe prawa i wolności osoby, której dane dotyczą są nadrzędne wobec**	☐ tak

	interesu Administratora Danych lub strony trzeciej? *Udzielając odpowiedzi należy wziąć pod uwagę całokształt okoliczności przetwarzania wynikający z udzielonych w Teście odpowiedzi.* *Odpowiedź „tak" oznacza, że Administrator Danych nie może zastosować przesłanki prawnie uzasadnionego interesu z art. 6 ust. 1 lit. f RODO.* *Należy zaznaczyć odpowiedz „tak" zawsze wtedy, gdy osoba której dane dotyczą jest dzieckiem.*	☐ nie Uzasadnienie: …
20.	**Czy Administrator Danych może przetwarzać dane osobowe w ramach opisanej operacji przetwarzania na podstawie art. 6 ust. 1 lit. f RODO?**	☐ tak ☐ nie Uzasadnienie: …
21.	**Rekomendacje** *Jeżeli wynik testu równowagi jest negatywny dla Administratora Danych, należy określić rekomendacje w zakresie dalszego przetwarzania danych osobowych.* *Rekomendacje mogą dotyczyć, w szczególności:* *- wdrożenia odpowiednich środków naprawczych mających wpływ na wzajemne interesy Administratora Danych lub stron trzecich i osoby, której dane dotyczą,* *- zmiany podstawy prawnej przetwarzania danych osobowych w procesie,* *- zaprzestania przetwarzania danych osobowych w procesie.*	

Załącznik (*opcjonalnie*):

1) *Opis stosowanych zabezpieczeń*

…….....

Data i podpis OBDO

OPIS STOSOWANYCH ZABEZPIECZEŃ		
ZABEZPIECZENIA ORGANIZACYJNE		
1.	**Imię, nazwisko oraz stanowisko osoby udzielającej odpowiedzi na pytania** *Ta część powinna zostać uzupełniona przez osobę (osoby) posiadającą wiedzę na temat stosowanych zabezpieczeń organizacyjnych ochrony danych osobowych*	
2.	**Czy wyznaczono osobę odpowiedzialną za ochronę danych osobowych** *Należy wskazać, czy w strukturze Administratora Danych wyznaczono osobę odpowiedzialną za ochronę danych osobowych*	☐ wyznaczono Inspektora Ochrony Danych ☐ wyznaczono inną osobę (*należy wskazać jaką*): … ☐ brak
3.	**Kompetencje osoby odpowiedzialnej za ochronę danych osobowych** *Należy wskazać jakie kompetencje ma osoba odpowiedzialna za ochronę danych osobowych w strukturze Administratora Danych*	☐ doświadczenie zawodowe w obszarze ochrony danych osobowych, lata doświadczenia … ☐ wykształcenie kierunkowe (np. prawnicze, informatyczne) (*jakie*): … ☐ studia podyplomowe w zakresie ochrony danych osobowych ☐ studia podyplomowe w zakresie bezpieczeństwa informacji ☐ certyfikaty ISO (*jakie*): … ☐ inne (*jakie*): …
4.	**Czy wyznaczono osobę odpowiedzialną za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych** *Należy wskazać, czy w strukturze Administratora Danych wyznaczono osobę odpowiedzialną za ochronę danych osobowych w systemach informatycznych*	☐ wyznaczono Administratora Systemów Informatycznych ☐ wyznaczono inną osobę (*należy wskazać jaką*): … ☐ brak

5.	**Dokumentacja ochrony danych osobowych** *Należy wskazać które z wymienionych dokumentów / procedur zostały wdrożone i są stosowane w strukturze Administratora Danych*	Polityka ochrony danych osobowych: ☐ tak ☐ nie Rejestr czynności przetwarzania: ☐ tak ☐ nie ☐ nie dotyczy Rejestr kategorii czynności przetwarzania: ☐ tak ☐ nie ☐ nie dotyczy Zasady privacy by design oraz privacy by default: ☐ tak ☐ nie Zasady retencji danych osobowych: ☐ tak ☐ nie Procedura szkoleń oraz nadawania upoważnień do przetwarzania danych osobowych: ☐ tak ☐ nie Procedura postępowania z incydentami ochrony danych osobowych: ☐ tak

		☐ nie Procedura oceny skutków dla ochrony danych osobowych (*data protection impact assessment*): ☐ tak ☐ nie Procedura realizacji praw osób, których dane dotyczą: ☐ tak ☐ nie Procedura tworzenia kopii zapasowych: ☐ tak ☐ nie Procedury IT (np. procedury odtwarzania systemu po awarii, procedury testowania systemów, etc.): ☐ tak (*jakie*): … ☐ nie
6.	**Szkolenia** *Należy wskazać czy Administrator Danych szkoli pracowników/ współpracowników z zasad ochrony danych osobowych, a jeśli taki w jaki sposób są przeprowadzane np. w formie elektronicznej (e-learning), stacjonarnej, zdalnej (za pośrednictwem narzędzi do komunikacji na odległość)*	☐ tak *(w jaki sposób)*: … ☐ nie
		…….....
		Data i podpis osoby udzielającej odpowiedzi na pytania

OPIS STOSOWANYCH ZABEZPIECZEŃ		
ZABEZPIECZENIA FIZYCZNE *dotyczy pomieszczeń w których będą/ mogą być przetwarzane dane w procesie, którego dotyczy Test*		
1.	**Imię, nazwisko oraz stanowisko osoby udzielającej odpowiedzi na pytania** *Ta część powinna zostać uzupełniona przez osobę (osoby) posiadającą wiedzę na temat stosowanych zabezpieczeń fizycznych dotyczących pomieszczeń w których będą / mogą być przetwarzane dane w procesie, którego dotyczy Test.*	
2.	**Zabezpieczenia pomieszczeń** *Należy określić stosowane zabezpieczenia w pomieszczeń w których będą / mogą być przetwarzane dane.*	Dostęp do pomieszczeń ☐ Klucze, ☐ Karty magnetyczne/ karty chipowe ☐ Ochrona obiektu przez firmę ochroniarską, ☐ Systemy alarmowe ☐ Kamery monitoringu CCTV Pozostałe środki ☐ Zamykane szafy/ szuflady, ☐ Systemy przeciwpożarowe, ☐ Niszczarki na dokumenty/ dedykowane pojemniki do bezpiecznego niszczenia dokumentów, ☐ inne (*jakie*): …
4.	**Zabezpieczenia serwerowni** *Należy określić stosowane zabezpieczania w odniesieniu do pomieszczenia serwerowni.*	Dostęp do pomieszczeń ☐ Klucze, ☐ Karty magnetyczne/ karty chipowe

		☐ Ochrona przez firmę ochroniarską, ☐ Systemy alarmowe ☐ Kamery monitoringu CCTV <u>Pozostałe środki</u> ☐ Systemy przeciwpożarowe, ☐ inne (*jakie*): …
		…….....
		Data i podpis osoby udzielającej odpowiedzi na pytania

OPIS STOSOWANYCH ZABEZPIECZEŃ		
ZABEZPIECZENIA TECHNICZNE *dotyczy narzędzi informatycznych które będą/ mogą być wykorzystywane do przetwarzania danych w procesie którego dotyczy Test*		
1.	**Imię, nazwisko oraz stanowisko osoby udzielającej odpowiedzi na pytania** *Ta część powinna zostać uzupełniona przez osobę (osoby) posiadającą wiedzę na temat stosowanych zabezpieczeń technicznych dotyczących narzędzi informatycznych które będą/ mogą być wykorzystywane do przetwarzania danych w procesie którego dotyczy Test*	
2.	**Stosowane zabezpieczenia**	☐ zapora firewall, ☐ indywidualny login i hasło dla każdego użytkownika, ☐ uprawnienia dostępu dostosowane do potrzeb użytkowników ☐ szyfrowanie, ☐ pseudonimizacja ☐ tworzenie kopii zapasowych ☐ zasilanie awaryjne (UPS), ☐ ochrona antywirusowa, ☐IDS/IPS ☐ mechanizm odnotowywania logów systemowych ☐ inne *(jakie)* …
		…….....
		Data i podpis osoby udzielającej odpowiedzi na pytania

Załącznik nr 9 – Procedura realizacji praw osób, których dane dotyczą

1. Każda osoba, której dane dotyczą, ma prawo do wystąpienia do Administratora Danych z żądaniem realizacji praw przysługujących jej w związku przetwarzaniem jej danych osobowych. W szczególności dotyczy to prawa do:
   1.1. wycofania wyrażonej zgody na przetwarzanie danych osobowych (art. 7 ust. 3 RODO),
   1.2. dostępu do danych osobowych (art. 15 RODO),
   1.3. sprostowania danych osobowych (art. 16 RODO),
   1.4. usunięcia danych osobowych (w tym prawa do bycia zapomnianym) (art. 17 RODO),
   1.5. ograniczenia przetwarzania danych osobowych (art. 18 RODO),
   1.6. przenoszenia danych osobowych (art. 20 RODO),
   1.7. wniesienia sprzeciwu wobec przetwarzania danych osobowych (art. 21 RODO),
   1.8. niepodlegania decyzjom opartym wyłącznie na zautomatyzowanym przetwarzaniu danych osobowych (art. 22 RODO).
2. Osoba, której dane dotyczą może wnieść swoje żądanie w dowolnej formie (papierowej, ustnej lub elektronicznej).
3. Żądanie realizacji praw może zostać również złożone za pośrednictwem podmiotu przetwarzającego, któremu Administrator Danych powierzył przetwarzanie danych osobowych. W takich przypadkach, podmiot przetwarzający informuje Administratora Danych o wniesieniu żądania zgodnie z postanowieniami zawartej umowy powierzenia przetwarzania danych osobowych.
4. Pracownik, do którego wpłynęło żądanie realizacji praw, jest zobowiązany do:
   4.1. poinformowania osoby składającej żądanie o jego przyjęciu i przekazaniu do rozpoznania,
   4.2. weryfikacji / potwierdzenia tożsamości osoby występującej z tym żądaniem,
   4.3. przekazania żądania do OBDO.
5. Jeżeli pracownik, do którego wpłynęło żądanie, ma uzasadnione wątpliwości co do tożsamości osoby, od której to żądanie pochodzi, może zażądać od niej dodatkowych informacji niezbędnych do potwierdzenia jej tożsamości.
6. Poinformowania o przyjęciu żądania oraz weryfikacji tożsamości osoby występującej z żądaniem dokonuje się w tej samej formie w jakiej zostało złożone żądanie.
7. Pracownik, do którego wpłynęło żądanie realizacji praw przekazuje je do OBDO:
   7.1. bezpośrednio
   7.2. niezwłocznie, jednak nie później niż w terminie 48 godzin od jego otrzymania.
8. Po otrzymaniu żądania realizacji praw, OBDO dokonuje jego analizy, a w szczególności ustala:

8.1. jaki jest zakres żądania,

8.2. czy dane osobowe, których dotyczy żądanie są przetwarzane przez Administratora Danych,

8.3. czy w odniesieniu do danych osobowych, których dotyczy żądanie Administrator Danych występuje w roli ich administratora w rozumieniu art. 4 pkt 7 RODO, czy też w roli podmiotu przetwarzającego, w rozumieniu art. 4 pkt 8 RODO,

8.4. czy dane prawo przysługuje osobie występującej z żądaniem.

9. W toku analizy, o której mowa w pkt 7, OBDO konsultuje się z osobami merytorycznie zaangażowanymi w proces przetwarzania danych osobowych osoby występującej z żądaniem.

10. Jeżeli w toku analizy pojawią się uzasadnione wątpliwości co do zakresu zgłoszonego żądania, w szczególności, gdy z uwagi na treść żądania nie jest oczywiste, z którego z praw osoba, której dane dotyczą chce skorzystać, OBDO na podstawie zebranych informacji przygotowuje odpowiedź z prośbą o skonkretyzowanie żądań.

11. Jeżeli w toku dalszej analizy, stwierdzone zostanie, że:

11.1. Administrator Danych nie przetwarza danych osobowych stanowiących przedmiot żądania,

11.2. dane prawo nie przysługuje osobie występującej z żądaniem,

OBDO przygotowuje odpowiedź odmowną realizacji prawa.

12. Odpowiedź odmowna realizacji prawa przekazywana jest osobie, która wniosła żądanie niezwłocznie, najpóźniej w terminie miesiąca od otrzymania żądania. Odpowiedź odmowna zawiera, w szczególności informacje o:

12.1. samym fakcie niespełnienia żądania,

12.2. powodach niespełnienia żądania,

12.3. możliwości wniesienia skargi do organu nadzorczego,

12.4. możliwości skorzystania ze środków ochrony prawnej przed sądem.

13. Jeżeli w toku analizy, stwierdzone zostanie, że dane prawo przysługuje osobie występującej z żądaniem lub przysługuje jej w określonym zakresie, OBDO w porozumieniu z osobami merytorycznie zaangażowanymi w proces przetwarzania danych osobowych:

13.1. ustala sposób realizacji prawa,

13.2. przygotowuje odpowiedź wskazującą na sposób realizacji prawa.

14. Przekazywanie odpowiedzi na żądanie realizacji praw oraz prowadzenie jakiejkolwiek komunikacji z osobami, których dane dotyczą, odbywa się w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.

15. Odpowiedzi przekazuje się w formie pisemnej lub elektronicznej. Przekazanie informacji w formie ustnej może nastąpić wyłącznie wtedy, gdy osoba, której dane dotyczą, tego zażąda i to wyłącznie pod takim warunkiem, że innymi sposobami potwierdzi się jej tożsamość.

16. Spełnienie żądania realizacji prawa następuje bez zbędnej zwłoki, nie później jednak niż w terminie jednego miesiąca od dnia otrzymania żądania.

17. Termin, o którym mowa w pkt 16 może zostać przedłużony o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań pochodzących od tej samej osoby. W terminie miesiąca od otrzymania żądania, informuje się osobę, której dane dotyczą, o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia.

18. OBDO prowadzi rejestr zgłoszonych żądań realizacji praw, według wzoru, który znajduje się w niniejszym Załączniku.

19. Podejmowanie działań w związku z realizacją praw osób, których dane dotyczą jest co do zasady wolne od opłat.

20. Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, Administrator Danych może:

    20.1. pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań, albo

    20.2. odmówić podjęcia działań w związku z żądaniem.

21. Działania osoby, której dane dotyczą, o których mowa w pkt 20 mają charakter nadużycia prawa, przez co należy rozumieć korzystanie z prawa i używanie instrumentów służących jego realizacji nie w celu zrealizowania wartości, którym to prawo ma służyć, chociaż z powoływaniem się na nie. W szczególności, za nadużycie prawa do informacji na gruncie RODO należy uznać takie działania osób, których dane dotyczą, które:

    21.1. nie służą realizacji prawa do ochrony danych osobowych oraz

    21.2. są nieuzasadnione lub nadmierne.

22. OBDO dokonuje oceny, czy zostały spełnione przesłanki, o których mowa w pkt 21 tj. czy działania osoby, której dane dotyczą można uznać za nadużycie prawa.

23. Dokonana ocena, przedkładana jest Administratorowi Danych przez Koordynatora ds. ochrony danych osobowych. Na jej podstawie Administrator Danych podejmuje ostateczną decyzję o nałożeniu opłaty lub odmowie podjęcia działań.

24. Ogólne zasady realizacji poszczególnych praw osób, których dane dotyczą znajdują się poniżej w niniejszym Załączniku.

Prawo do wycofania zgody (art. 7 RODO)

1. W sytuacji, jeżeli przetwarzanie danych odbywa się na podstawie zgody osoby, której dane dotyczą, osoba ta ma prawo do jej odwołania w dowolnym momencie.

2. Skutkiem odwołania zgody jest brak możliwości przetwarzania danych osobowych z powołaniem się na tę właśnie podstawę przetwarzania danych w przyszłości.

3. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.

Prawo dostępu do danych (art. 15 RODO)

1. Prawo dostępu do danych daje osobie, której dane dotyczą prawo do:

   1.1. uzyskania od Administratora Danych potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli tak, również dodatkowych informacji dotyczących tego przetwarzania (m.in. w zakresie celu przetwarzania, kategorii przetwarzanych danych, kategorii odbiorców jej danych osobowych, etc.),

   1.2. uzyskania kopii danych osobowych podlegających przetwarzaniu.

2. Osoba, której dane dotyczą może wedle swego uznania, choć w ramach katalogu zamkniętego określonego w art. 15 RODO, kształtować zakres uzyskanych informacji czy danych przekazanych w postaci kopii. Realizując przyznane uprawnienia, może więc żądać przekazania zarówno każdej, jak i wszystkich wskazanych w art. 15 RODO informacji, jak również żądać kopii czy wglądu do wybranych bądź wszystkich danych.

3. Rezultatem wykonania prawa dostępu do danych osobowych powinno być udzielenie osobie, której dane dotyczą, żądanych przez nią informacji.

4. W wyniku realizacji prawa dostępu do danych osobowych, osoba, której dane dotyczą, może uzyskać kopię danych osobowych we wskazanym przez siebie formacie. Jeżeli jednak nie zastrzeże tego formatu w swoim żądaniu informacje powinny zostać przekazane za pomocą tego samego środka porozumiewania się, przy użyciu, którego osoba, której dane dotyczą, skierowała swoje żądanie do Administratora Danych.

Prawo do sprostowania danych (art. 16 RODO)

1. Osoba, której dane dotyczą posiada uprawnienie do:

   1.1. sprostowania nieprawidłowych danych osobowych,

   1.2. uzupełnienia niekompletnych danych osobowych.

2. Osoba, której dane dotyczą swoim żądaniem powinna wykazać, że jej żądanie jest w istocie zasadne tj. Administrator Danych przetwarza dane nieprawidłowe lub niekompletne.

3. Tylko po spełnieniu warunku wskazanego w pkt 2 Administrator Danych będzie zobowiązany do niezwłocznego sprostowania danych nieprawidłowych lub do uzupełnienia danych niekompletnych.

4. Zgodnie z art. 19 RODO Administrator Danych informuje o sprostowaniu każdego odbiorcę, któremu ujawniono dane osobowe, chyba, że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.

Prawo do usunięcia danych (art. 17 RODO)

1. Prawo do usunięcia danych składa się z dwóch uprawnień cząstkowych:

1.1. możliwości żądania usunięcia danych osobowych przez Administratora Danych,

1.2. możliwości żądania, aby Administrator Danych poinformował innych administratorów danych, którym upublicznił dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje (tzw. prawo do zapomnienia).

2. Możliwość skorzystania z uprawnienia do żądania usunięcia danych przez innych administratorów jest uzależniona od możliwości skorzystania z żądania usunięcia danych osobowych przez pierwotnego Administratora Danych.

3. Osoba, której dane dotyczą, może żądać usunięcia swoich danych osobowych we wskazanych w art. 17 ust. 1 RODO przypadkach, tj. m.in. w sytuacji, jeżeli jej dane osobowe nie są już niezbędne do celów, w których były przetwarzane, wycofała ona zgodę na przetwarzanie danych, wniosła sprzeciw od takiego przetwarzania, czy też jej dane przetwarzane były niezgodnie z prawem.

4. Przez usunięcie danych osobowych należy rozumieć całkowite zniszczenie danych (w tym nośników, na których były one zapisane) lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą (tzw. anonimizacja danych). Efektem działania Administratora Danych powinien być brak możliwości dalszego dokonywania jakichkolwiek operacji na tych danych.

5. W przypadku prawa do bycia zapomnianym mamy do czynienia jedynie z obowiązkiem informacyjnym Administratora Danych wobec innych administratorów. Administrator Danych nie ma obowiązku dopilnowania, aby dane faktycznie zostały przez tych administratorów usunięte. Dodatkowo zakres obowiązku poinformowania innych administratorów jest ograniczony przez: dostępną technologię, koszt realizacji obowiązku poinformowania, odwołanie do podejmowania rozsądnych działań w wykonaniu tego obowiązku.

Prawo do ograniczenia przetwarzania (art. 18 RODO)

1. Osoba, której dane dotyczą ma prawo do żądania ograniczenia przetwarzania danych osobowych. Ograniczenie przetwarzania danych osobowych polega na konieczności ograniczenia przetwarzania danych wyłącznie do ich przechowywania.

2. Administrator Danych jest zobowiązany do ograniczenia przetwarzania danych, jeżeli zaistnieje jedna ze wskazanych w art. 18 RODO przesłanek, tj. osoba, której dane dotyczą:

2.1. kwestionuje prawidłowość danych osobowych (ograniczenie przetwarzania następuje automatycznie na okres pozwalający Administratorowi Danych sprawdzić prawidłowość tych danych),

2.2. sprzeciwia się usunięciu danych osobowych przetwarzanych niezgodnie z prawem,

2.3. żąda zastosowania ograniczenia przetwarzania w stosunku do danych, które powinny zostać usunięte, ale które są jej niezbędne do ustalenia, dochodzenia lub obrony przysługujących jej roszczeń,

2.4. wniosła sprzeciw wobec przetwarzania danych osobowych (ograniczenie przetwarzania następuje automatycznie, na okres pozwalający Administratorowi Danych stwierdzić czy sprzeciw jest zasadny).

3. Przykładami ograniczenia przetwarzania są:

3.1. czasowe przeniesienie wybranych danych osobowych do innego systemu przetwarzania,

3.2. uniemożliwienie użytkownikom dostępu do wybranych danych,

3.3. czasowe usunięcie opublikowanych danych ze strony internetowej.

4. W każdym przypadku, dane, w odniesieniu do których ograniczono przetwarzanie, powinny być wyraźnie odróżnione od pozostałych danych oraz nie mogą podlegać dalszemu przetwarzaniu ani modyfikacjom.

Prawo do przenoszenia danych (art. 20 RODO)

1. Osobie, której dane dotyczą przysługuje prawo do przenoszenia danych, na które składają się dwa uprawnienia:

1.1. prawo otrzymania przez osobę, której dane dotyczą, w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, danych osobowych jej dotyczących, które dostarczyła Administratorowi Danych,

1.2. prawo przesłania przez osobę, której dane dotyczą, danych osobowych jej dotyczących, które dostarczyła Administratorowi Danych, innemu administratorowi, bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe.

2. Uprawnienia, o których mowa w pkt 1 mogą być wykonywanie niezależnie od siebie i niezależnie od uprawnienia do uzyskania kopii danych osobowych podlegających przetwarzaniu.

3. Osoba, której dane dotyczą, może skorzystać z prawa do przenoszenia danych osobowych, jeżeli łącznie spełnione są dwa warunki:

3.1. przetwarzanie danych odbywa się na podstawie zgody lub w celu wykonania umowy, oraz

3.2. przetwarzanie danych odbywa się w sposób zautomatyzowany (prawo do przenoszenia danych nie obejmuje tzw. zbiorów papierowych).

4. Prawo do przenoszenia danych obejmuje dane osobowe dotyczące osoby, która wykonuje to prawo, które to dane ta osoba świadomie i aktywnie przekazała. Nie obejmuje natomiast danych wywnioskowanych przez Administratora Danych w procesie ich przetwarzania.

Prawo do wniesienia sprzeciwu (art. 21 RODO)

1. Osoba, której dane dotyczą, ma prawo do wniesienia sprzeciwu wobec przetwarzania jej danych osobowych:

1.1. opartego na interesie publicznym lub prawnie uzasadnionych interesach, w tym wobec profilowania na podstawie tych przepisów, z przyczyn związanych z jej szczególną sytuacją,

1.2. na potrzeby marketingu bezpośredniego,

1.3. do celów badań naukowych lub historycznych lub do celów statystycznych, z przyczyn związanych z jej szczególną sytuacją.

2. W razie otrzymania skutecznego sprzeciwu wobec przetwarzania danych osobowych, Administrator Danych powinien niezwłocznie zaprzestać przetwarzania danych w zakresie objętym tym sprzeciwem.

3. Jeżeli Administrator Danych uzna sprzeciw za pozbawiony podstaw, w szczególności z takiej przyczyny, że w jego ocenie nie zachodzi szczególna sytuacja uzasadniająca wniesienie sprzeciwu, ewentualny nakaz uwzględnienia sprzeciwu może zostać wydany przez organ nadzorczy na skutek skargi wniesionej przez zainteresowaną osobę.

Prawo do niepodlegania zautomatyzowanym decyzjom (art. 22 RODO)

1. Osoba, której dane dotyczą ma prawo do niepodlegania decyzji opartej wyłącznie na zautomatyzowanym przetwarzaniu danych osobowych, w tym na profilowaniu. Prawo to dotyczy sytuacji, w których zautomatyzowane podejmowanie decyzji:

1.1. wywołuje skutki prawne wobec osoby, której dane dotyczą,

1.2. wpływa istotnie na osobę, której dane dotyczą, w podobny sposób do skutków prawnych.

2. Podejmowanie przez Administratora Danych zautomatyzowanych decyzji, o których mowa w pkt 1, możliwe jest tylko pod warunkiem, że:

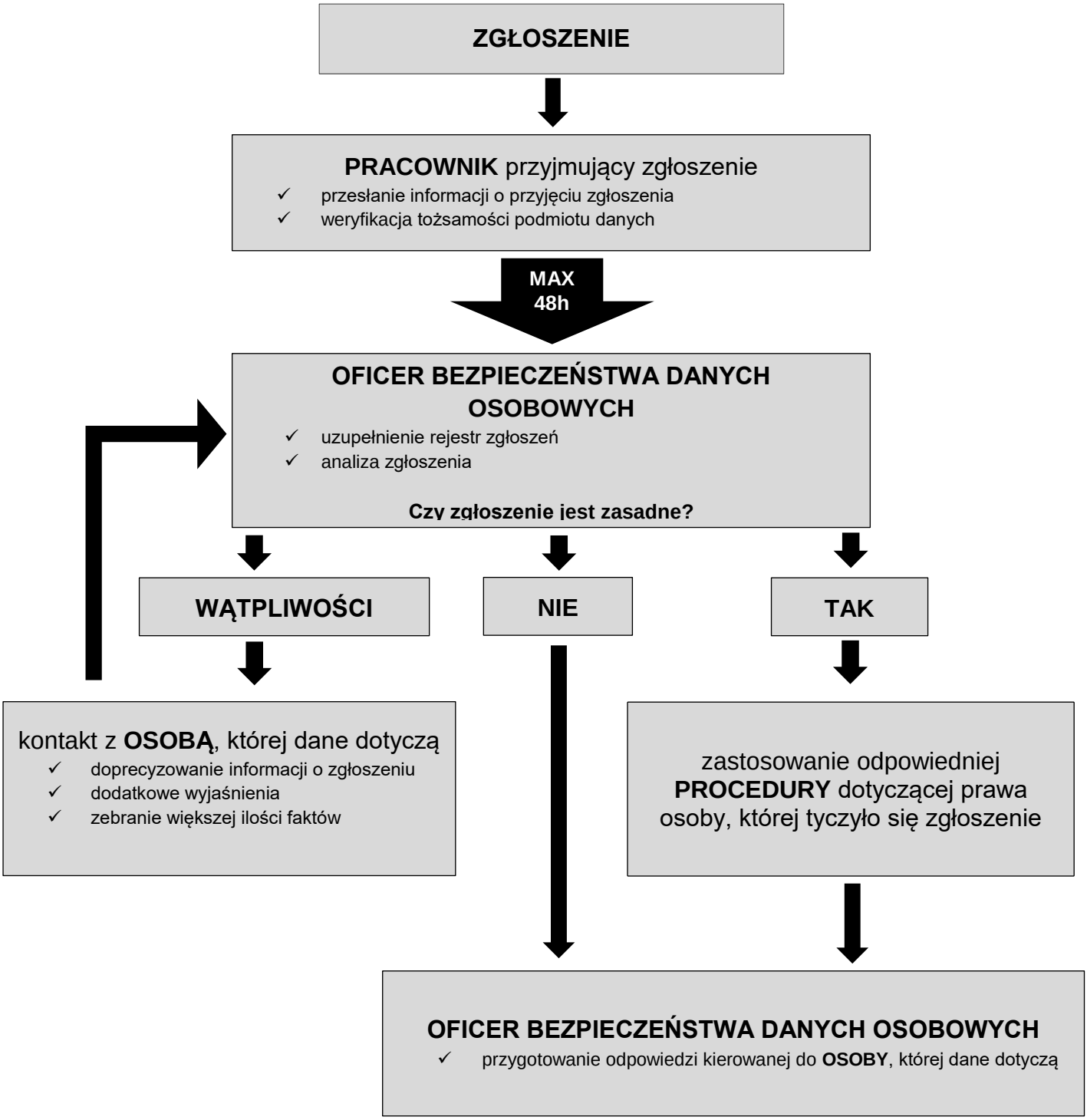
2.1. jest ono niezbędne do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a Administratorem Danych,

2.2. jest dozwolone prawem Unii lub prawem państwa członkowskiego,

2.3. opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

3. Jeżeli automatyczne podejmowanie decyzji jest niezbędne do zawarcia lub wykonania umowy albo gdy odbywa się na podstawie wyraźnej zgody, Administrator Danych powinien wdrożyć właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, o co najmniej prawa do uzyskania interwencji ludzkiej, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji. Oznacza to konieczność zapewnienia możliwości odwołania się osoby, której dane dotyczą, od automatycznego rozstrzygnięcia. Takie odwołanie powinno być rozpatrywane przez człowieka.

Schemat graficzny procedury



Wzór rejestru zgłoszonych żądań realizacji praw

Lp.	Numer żądania	Data wpływu żądania *(dd/mm/rrrr)*	Osoba, której dane dotyczą *(imię, nazwisko, ew. inne dane identyfikujące)*	Przedmiot żądania	Data wysłania odpowiedzi na żądanie *(dd/mm/rrrr)*	Rodzaj odpowiedzi *(realizacja prawa / odmowa realizacji prawa / częściowa realizacja prawa)*
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						

Załącznik nr 10 – Wzór sprawozdania z audytu zgodności przetwarzania danych osobowych

SPRAWOZDANIE Z AUDYTU ZGODNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH Z PRZEPISAMI O OCHRONIE DANYCH OSOBOWYCH

……

miejscowość, data

1. Administrator Danych: ……..……..…….

2. Oficer Bezpieczeństwa Danych Osobowych: ……..……..……

3. Data rozpoczęcia audytu: ……..……..……

4. Data zakończenia audytu: ……..……..……

5. Przedmiot audytu:

……..……

……..……

6. Zakres audytu:

……..……

……..……

7. Wykaz czynności podjętych w toku audytu:

……..……

……..……

8. Opis stanu faktycznego stwierdzonego w toku audytu oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych:

……..……

……..……

9. Stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych w zakresie objętym audytem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem:

LP.	STWIERDZONY PRZYPADEK NARUSZENIA	DZIAŁANIA PRZYWRACAJĄCE STAN ZGODNY Z PRAWEM / REKOMENDACJE	
		DZIAŁANIA OBDO	DZIAŁANIA ADMINISTRATORA DANYCH
1.			
2.			
3.			

10. Załączniki:

.....

Data i podpis

Oficera Bezpieczeństwa Danych Osobowych

Otrzymują:

1 x oryginał Administrator Danych

1 x kopia Oficer Bezpieczeństwa Danych Osobowych

Załącznik nr 11 – Procedura kontroli podmiotów przetwarzających

1. Administrator Danych dopuszcza, by dane osobowe, których jest administratorem w rozumieniu art. 4 pkt 7 RODO, były przetwarzane poza jego strukturami organizacyjnymi przez podmioty przetwarzające.
2. Przetwarzanie danych osobowych przez podmioty przetwarzające może się odbywać wyłącznie w określonym celu i zakresie, na mocy umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego.
3. Administrator Danych ma prawo kontroli podmiotów przetwarzających, którym powierzył przetwarzanie danych osobowych z punktu widzenia zgodności tego przetwarzania z:
   3.1. przepisami prawa,
   3.2. postanowieniami zawartej umowy powierzenia przetwarzania danych osobowych,
   3.3. wytycznymi i rekomendacjami organów nadzorczych oraz organów doradczych w zakresie ochrony danych i prywatności.
4. Kontrola, o której mowa w pkt 3 prowadzona jest w postaci audytu podmiotu przetwarzającego.
5. Szczegóły dotyczące audytu podmiotu przetwarzającego określa zawarta z tym podmiotem umowa powierzenia przetwarzania danych osobowych. W szczególności, dotyczy to postanowień w zakresie sposobu i terminu przekazywania podmiotowi przetwarzającemu informacji o terminie i zakresie audytu.
6. W sytuacji, gdy umowa powierzenia przetwarzania danych osobowych nie określa sposobu i terminu przekazywania podmiotowi przetwarzającemu informacji o terminie i zakresie audytu, kwestie te ustalane są z tym podmiotem w formie porozumienia przed przeprowadzeniem pierwszego audytu, z zastrzeżeniem, że poczynione ustalenia pozostają właściwe dla przyszłych audytów.
7. Audyt podmiotu przetwarzającego może zostać przeprowadzony, w szczególności w następujących przypadkach:
   7.1. powierzenie przetwarzania obejmuje szczególne kategorie danych osobowych i/lub dane osobowe dotyczące wyroków skazujących oraz naruszeń prawa,
   7.2. powierzenie przetwarzania obejmuje dane osobowe osób poniżej 16 r.ż.,
   7.3. powierza się przetwarzanie danych osobowych na dużą skalę,
   7.4. Administrator Danych otrzymał informację o incydentach z zakresu ochrony danych osobowych występujących u podmiotu przetwarzającego.
8. Decyzję o przeprowadzeniu audytu podmiotu przetwarzającego podejmuje Administrator Danych:
   8.1. samodzielnie,
   8.2. na podstawie złożonego wniosku o przeprowadzenie audytu.
9. Z wnioskiem o przeprowadzenie audytu podmiotu przetwarzającego może wystąpić:
   9.1. OBDO,

9.2. Osoby zarządzające procesami przetwarzania danych osobowych.

10. Wniosek o przeprowadzenie audytu podmiotu przetwarzającego składany jest do Administratora Danych.

11. Wniosek o przeprowadzenia audytu podmiotu przetwarzającego zawiera co najmniej:

    11.1. nazwę oraz siedzibę podmiotu przetwarzającego,

    11.2. uzasadnienie konieczności przeprowadzenia audytu.

12. Na podstawie otrzymanego wniosku, Administrator Danych podejmuje ostateczną decyzję o przeprowadzeniu audytu podmiotu przetwarzającego. Gdy jest to zasadne, przed podjęciem decyzji, Administrator Danych konsultuje się z OBDO.

13. Audyt podmiotu przetwarzającego realizowany jest przez OBDO. Jeżeli jest to zasadne, OBDO realizuje audyt przy współpracy z innymi osobami upoważnionymi przez Administratora Danych, których wiedza może mieć kluczowe znaczenie dla merytorycznej poprawności przeprowadzanego audytu.

14. Audyt podmiotu przetwarzającego realizowany jest:

    14.1. w siedzibie podmiotu przetwarzającego,

    14.2. w głównym miejscu przetwarzania powierzonych danych osobowych, lub

    14.3. zdalnie.

15. OBDO, Osoba zarządzająca procesami przetwarzania danych osobowych oraz osoba odpowiedzialna za bezpośrednią współpracę i utrzymywanie stałych kontaktów z podmiotem przetwarzającym opracowują wspólnie harmonogram przeprowadzania audytu, który wskazuje w szczególności na:

    15.1. termin audytu,

    15.2. miejsce audytu,

    15.3. zakres audytu,

    15.4. osoby biorące udział w audycie.

16. OBDO, przy współpracy z osobą odpowiedzialną za bezpośrednią współpracę i utrzymywanie stałych kontaktów z podmiotem przetwarzającym, informuje ten podmiot o terminie, miejscu i zakresie audytu.

17. OBDO przeprowadza audyt z wykorzystaniem formularza audytu, którego wzór znajduje się w niniejszym Załączniku.

18. Formularz audytu uzupełniany jest:

    18.1. w przypadku audytu w siedzibie podmiotu przetwarzającego lub w głównym miejscu przetwarzania powierzonych danych osobowych – przez OBDO oraz inne osoby realizujące audyt, o których mowa w pkt 14,

    18.2. w przypadku audytu zdalnego – przez osoby upoważnione do tego przez podmiot przetwarzający.

19. Po przeprowadzonym audycie OBDO sporządza Protokół poaudytowy, według wzoru znajdującego się w niniejszym Załączniku.

20. OBDO przedkłada Protokół poaudytowy

    20.1. Administratorowi Danych,

    20.2. podmiotowi przetwarzającemu.

21. Podmiot przetwarzający ma 7 dni na ustosunkowanie się do treści przedstawionego mu Protokołu poaudytowego, z zastrzeżeniem, że umowa powierzenia przetwarzania danych osobowych zawarta z tym podmiotem może określać inny termin.

22. Jeżeli w wyniku audytu stwierdzono niezgodność przetwarzania powierzonych danych osobowych z:

    22.1. obowiązującymi przepisami prawa, lub

    22.2. postanowieniami zawartej umowy powierzenia przetwarzania danych osobowych,

    22.3. wytycznymi i rekomendacjami organów nadzorczych oraz organów doradczych w zakresie ochrony danych i prywatności,

    Administrator Danych, na podstawie przedłożonego mu Protokołu poaudytowego, podejmuje ostateczną decyzję w zakresie dalszej współpracy z podmiotem przetwarzającym.

23. Formularz audytu podmiotu przetwarzającego jest stosowany przez Administratora Danych również w stosunku do podmiotów, z którymi Administrator Danych chce nawiązać współpracę tj. potencjalnych podmiotów przetwarzających. W odniesieniu do takich podmiotów, niniejszą Procedurę kontroli podmiotów przetwarzających stosuje się odpowiednio z wyłączeniem pkt 5-6 oraz pkt 24.2.

FORMULARZ AUDYTU PODMIOTU PRZETWARZAJĄCEGO			
Administrator Danych		**Nazwa:** **Siedziba:**	
Podmiot przetwarzający		**Nazwa:** **Siedziba:**	
Data i miejsce audytu **w przypadku audytu zdalnego należy wskazać datę uzupełnienia Formularza*			
Osoby reprezentujące podmiot przetwarzający biorące udział w audycie **w przypadku audytu zdalnego należy wskazać osoby odpowiedzialne za uzupełnienie Formularza*		1. *…(imię, nazwisko, stanowisko, dane kontaktowe)…* 2. *…(imię, nazwisko, stanowisko, dane kontaktowe)…* 3. *…(imię, nazwisko, stanowisko, dane kontaktowe)…*	
Osoby reprezentujące Administratora Danych biorące udział w audycie **w przypadku audytu zdalnego należy wskazać osoby do których Formularz jest wysyłany*		1. *…(imię, nazwisko, stanowisko, dane kontaktowe)…* 2. *…(imię, nazwisko, stanowisko, dane kontaktowe)…* 3. *…(imię, nazwisko, stanowisko, dane kontaktowe)…*	
Lp.	**Obszar**	**Pytania pomocnicze**	**Stan faktyczny**
1.	**Usługi świadczone na rzecz Administratora Danych**	1. Jaki jest rodzaj usług świadczonych przez podmiot przetwarzający, w związku z którymi dochodzi do powierzenia przetwarzania danych osobowych?	
2.	**Zakres przetwarzanych danych osobowych**	1. Kogo dane osobowe są przetwarzane?	
		2. Czy przetwarzane są dane osób poniżej 16 r.ż.?	

		3. Jakie kategorie danych osobowych są przetwarzane?	
		4. Czy przetwarzane są szczególne kategorie danych? (*jakie*)	
		5. Czy przetwarza się dane dotyczące wyroków skazujących i naruszeń prawa?	
3.	**Struktura organizacyjna**	1. Czy wyznaczono Inspektora Ochrony Danych? (*imię, nazwisko oraz dane kontaktowe*)	
		2. Jeżeli nie wyznaczono IOD, czy wyznaczono osobę o podobnym stanowisku, nadzorującą kwestie związane z ochroną danych osobowych? (*funkcja, imię, nazwisko oraz dane kontaktowe*)	
		3. Czy wyznaczono osobę odpowiedzialną za zabezpieczenia danych osobowych przetwarzanych za pomocą systemów informatycznych? (*imię, nazwisko, stanowisko oraz dane kontaktowe*)	
4.	**Polityki ochrony danych osobowych**	1. Jakie polityki w zakresie ochrony danych osobowych zostały wdrożone?	
		2. W jaki sposób polityki ochrony danych osobowych zostały wdrożone? (*np. formalnie zatwierdzone i wprowadzone w życie procedury dot. środków ochrony danych osobowych*)	
		3. Czy jest przeprowadzana regularna aktualizacja polityk ochrony danych osobowych?	
5.	**Audyt**	1. Czy wdrożono program audytowy obejmujący zgodność z regulacjami w zakresie ochrony danych osobowych?	
		2. Jeżeli tak, kto jest odpowiedzialny za przeprowadzanie audytów?	

		3. Jakie są metody przeprowadzania audytów, ich częstotliwość oraz zakres?	
6.	**Incydenty**	1. Czy wdrożono procedurę postępowania z incydentami z zakresu ochrony danych osobowych?	
		2. Czy osoby posiadające dostęp do powierzonych danych osobowych zostali przeszkoleni w zakresie zgłaszania incydentów z zakresu ochrony danych osobowych?	
		3. Czy w okresie ostatnich trzech lat miały miejsce incydenty z zakresu ochrony danych osobowych? (*rodzaj, ilość*)	
		4. Czy w okresie ostatnich trzech lat działalność podmiotu przetwarzającego była przedmiotem postępowania ze strony urzędów zajmujących się ochroną danych osobowych? (*rodzaj, ilość*)	
		5. Czy w okresie ostatnich trzech lat działalność podmiotu przetwarzającego była przedmiotem działań prawnych dotyczących zarzutów naruszenia prywatności lub ochrony danych osobowych? (*rodzaj, ilość*)	
		6. Czy w okresie ostatnich trzech lat podmiot przetwarzający zgłosił jakiekolwiek naruszenia bezpieczeństwa danych odpowiednim organom / urzędom (uwzględniając organy związane z ochroną danych osobowych) oraz / lub podmiotom zajmującym się ochroną danych osobowych?	
		7. Czy podmiot przetwarzający jest zdolny do powiadomienia Administratora Danych o jakimkolwiek naruszeniu bezpieczeństwa, które mogłoby mieć negatywne skutki dla ochrony	

		powierzonych do przetwarzania danych osobowych oraz praw i wolności osób, których te dane dotyczą, bez opóźnienia, tj. w ciągu 24 godzin od chwili powzięcia informacji o naruszeniu?	
7.	**Osoby posiadające dostęp do powierzonych danych osobowych w strukturze podmiotu przetwarzającego**	1. Czy stosuje się politykę lub procedurę ograniczającą dostęp do powierzonych danych osobowych?	
		2. W jaki sposób podejmowane są decyzje o tym, kto powinien otrzymać dostęp do powierzonych danych osobowych i w jaki sposób jest to sprawdzane i potwierdzane?	
		3. Jaka jest forma współpracy z osobami posiadającymi dostęp do powierzonych danych osobowych? (*umowa o pracę, umowa cywilnoprawna, umowa o współpracy*)	
		4. Czy osoby posiadające dostęp do powierzonych danych osobowych odbywają szkolenia w zakresie przetwarzania i ochrony prywatności danych oraz zgodności z przepisami prawa w zakresie ochrony danych osobowych? (*forma szkoleń, częstotliwość*)	
		5. Czy osobom posiadającym dostęp do powierzonych danych osobowych nadawane są upoważnienia do przetwarzania danych osobowych?	
		6. Czy osoby posiadające dostęp do powierzonych danych osobowych składają oświadczenia o zachowaniu tych danych w poufności przez okres trwania współpracy jak i po jej zakończeniu?	
		7. Czy prowadzona jest ewidencja osób posiadających dostęp do powierzonych danych	

		osobowych?	
		8. Czy w przypadku zakończenia współpracy z osobami posiadającymi dostęp do powierzonych danych osobowych, fizyczny i elektroniczny dostęp do powierzonych danych osobowych jest odbierany natychmiast po zakończeniu współpracy? (*sposób odbioru dostępu*)	
8.	**Forma przetwarzania powierzonych danych osobowych**	1. W jakiej formie przetwarzane są powierzone dane osobowe? (*papierowa, elektroniczna*)	
		2. Jeżeli dane osobowe przetwarzane są w formie elektronicznej, za pomocą systemów informatycznych, proszę podać nazwy tych systemów.	
9.	**Miejsce przetwarzania powierzonych danych osobowych**	1. W jakich lokalizacjach ma miejsce przetwarzanie powierzonych danych osobowych? (*dane osobowe przetwarzane na bieżąco, wersje archiwalne, kopie zapasowe*)	
		2. Czy jest prowadzona aktualna ewidencja dotycząca lokalizacji i przemieszczania sprzętu i nośników elektronicznych, które mogą zawierać powierzone dane osobowe?	
10.	**Podpowierzanie powierzonych danych osobowych**	1. Czy powierzone dane osobowe są podpowierzane innym podmiotom?	
		2. Jeżeli tak, jakim podmiotom i w jakim zakresie? (*nazwy podmiotów, zakres danych podpowierzanych poszczególnym podmiotom*)	
		3. Czy z podmiotami, którym podpowierza się dane osobowe zawarto umowę podpowierzenia?	
		4. Czy zawarta umowa podpowierzenia przewiduje nałożenie na podmiot, któremu dane są podpowierzane te same obowiązki ochrony danych	

		jakie zostały nałożone na podmiot przetwarzający na mocy umowy powierzenia z Administratorem Danych?	
		5. Czy podmiot przetwarzający monitoruje lub dokonuje audytu zgodności przetwarzania podpowierzonych danych osobowych z przepisami prawa oraz postanowieniami zawartej umowy podpowierzenia przetwarzania danych osobowych? (*zakres, częstotliwość audytów, metody, odpowiedzialność*)	
		6. Czy w przypadku zakończenia współpracy z podmiotem, któremu dane są podpowierzane, fizyczny i elektroniczny dostęp do powierzonych danych osobowych jest odbierany natychmiast po zakończeniu współpracy? (*sposób odbioru dostępu*)	
11.	**Udostępnianie powierzonych danych osobowych**	1. Czy powierzone dane osobowe są udostępniane innym podmiotom? (*zakres udostępnianych danych, nazwy podmiotów*)	
		2. Jeżeli tak, jakim podmiotom i w jakim zakresie? (*nazwy podmiotów, zakres danych udostępnianych poszczególnym podmiotom*)	
12.	**Przekazywanie powierzonych danych osobowych do państw trzecich**	1. Czy powierzone dane osobowe są przekazywane do państw trzecich?	
		2. Jeżeli tak, do jakich państw trzecich, jakim podmiotom, w jakim zakresie i na jakiej podstawie? (*państwo trzecie, nazwy podmiotów, zakres przekazywanych danych poszczególnym podmiotom, podstawa prawna*)	
13.	**Zabezpieczenia fizyczne**	1. Jakie zabezpieczenia fizyczne wdrożono dla ochrony powierzonych danych osobowych? **Należy opisać wdrożone zabezpieczenia fizyczne, w szczególności to jak zostały zabezpieczone pomieszczenia, w których*	

		przetwarzane są powierzone dane osobowe (polityki i procedury dostępu do pomieszczeń, rodzaj drzwi, rodzaj zamków, formy kontroli dostępu, formy zabezpieczenia przed osobami z zewnątrz, monitoring, ochrona, alarm, etc.) oraz to jak przechowuje się nośniki, na których przetwarzane są powierzone dane osobowe (rodzaje szaf, dane osobowe w formie papierowej (rodzaj szaf, zabezpieczenia fizyczne komputerów, niszczarki do dokumentów, etc.)	
14.	**Zabezpieczenia techniczne**	1. Jakie zabezpieczenia techniczne wdrożono dla ochrony powierzonych danych osobowych? **Należy opisać wdrożone zabezpieczenia techniczne, w szczególności jakie środki wdrożone zostały dla ograniczenia dostępu do powierzonych danych osobowych (kontrola dostępu poprzez ograniczanie uprawnień, indywidualny login i hasło, wymagania dotyczące złożoności hasła, okresowa kontrola uprawnień, etc.), jakie środki techniczne są stosowane do zapewnienia bezpieczeństwa systemu (antywirus, firewall, IPS, IDS, etc.), jakie środki wdrożone zostały dla zagwarantowania rozliczalności, poufności i integralności powierzonych danych osobowych*	
			…….....
			Data i podpis osoby wypełniającej Formularz

PROTOKÓŁ POAUDYTOWY NR .../……

……

miejscowość, data

1. Administrator Danych: ……..

2. Podmiot przetwarzający: ……..……..……..

3. Data rozpoczęcia audytu: ……..……..……..

4. Data zakończenia audytu: ……..……..……..

5. Miejsce audytu: ……..……

6. Osoby prowadzące czynności audytowe (*imiona, nazwiska, stanowiska*):

……..……..

7. Osoby upoważnione przez podmiot przetwarzający do udzielania wyjaśnień w trakcie czynności audytowych (*imiona, nazwiska, stanowiska*):

……..……..

8. Zakres audytu:

……..……..

9. Wykaz czynności podjętych w toku audytu:

……..……..

10. Wnioski poaudytowe:

……..……..

Kluczowe wnioski:

……..……..

Stwierdzone niezgodności przetwarzania powierzonych danych osobowych z obowiązującymi przepisami prawa:

……..……..

Stwierdzone niezgodności przetwarzania powierzonych danych osobowych z postanowieniami zawartej umowy powierzenia przetwarzania danych osobowych:

……

Stwierdzone niezgodności przetwarzania powierzonych danych osobowych z wytycznymi i rekomendacjami organów nadzorczych oraz organów doradczych w zakresie ochrony danych i prywatności

……

Rekomendacje:

……

11. Załączniki:

1) Formularz audytu podmiotu przetwarzającego z dnia …/…/……..

……

Data i podpis Oficera Bezpieczeństwa Danych Osobowych

Otrzymują:
1 x oryginał Administrator Danych
1 x kopia podmiot przetwarzający
1 x kopia Oficer Bezpieczeństwa Danych Osobowych

Załącznik nr 12 – Ogólny opis organizacyjnych środków bezpieczeństwa

ŚRODKI ORGANIZACYJNE		
LP.	**Stosowane środki organizacyjne**	**Uwagi**
1.	Osoby przetwarzające dane zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych.	
2.	Przeszkolono osoby przetwarzające dane osobowe w zakresie zabezpieczeń systemu informatycznego.	
3.	Osoby przetwarzające dane osobowe zostały zobowiązane do zachowania ich w tajemnicy.	
4.	Wyznaczono Oficera Bezpieczeństwa Danych Osobowych (OBDO).	
5.	Wyznaczono Administratora Systemów Informatycznych (ASI).	
6.	Opracowano i wdrożono Politykę ochrony danych osobowych.	
7.	Opracowano i wdrożono procedurę nadawania upoważnień do przetwarzania danych osobowych.	
8.	Wprowadzono ewidencję osób upoważnionych do przetwarzania danych osobowych.	
9.	Opracowano i wdrożono zasady retencji danych.	
10.	Opracowano i wdrożono procedurę postępowania z incydentami.	
11.	Opracowano i wdrożono procedury realizacji praw osób, których dane dotyczą.	
12.	Opracowano i wdrożono procedurę oceny skutków dla ochrony danych *(data protection impact assessment)*.	
13.	Opracowano i wdrożono procedury *privacy by design* oraz *privacy by default.*	
14.	Opracowano i wdrożono rejestr czynności przetwarzania administratora.	
15.	Opracowano i wdrożono rejestr kategorii czynności przetwarzania procesora.	

ŚRODKI OCHRONY FIZYCZNEJ		
LP.	**Stosowane środki ochrony fizycznej – zastosowane w zależności od lokalizacji**	**Uwagi**
1.	Pomieszczenia, w których przetwarzane są dane osobowe zabezpieczone zostały drzwiami zwykłymi.	
2.	Pomieszczenia, w których przetwarzane są dane osobowe zabezpieczone zostały drzwiami antywłamaniowymi.	
3.	Okna, w pomieszczeniach, w których przetwarzane są dane osobowe zabezpieczone zostały za pomocą krat.	
4.	Okna, w pomieszczeniach, w których przetwarzane są dane osobowe zabezpieczone zostały za pomocą rolet antywłamaniowych.	
5.	Okna, w pomieszczeniach, w których przetwarzane są dane osobowe zabezpieczone zostały za pomocą folii antywłamaniowej.	
6.	Pomieszczenia, w których przetwarzane są dane osobowe zabezpieczone zostały za pomocą alarmu przeciwwłamaniowego.	
7.	Pomieszczenia, w których przetwarzane są dane osobowe zabezpieczone zostały za pomocą systemu kontroli dostępu.	Recepcja / Rejestr wejść i wyjść / Identyfikatory tymczasowe dla odwiedzających / Identyfikatory dla pracowników / Karty dla pracowników
8.	Pomieszczenia, w których przetwarzane są dane osobowe zabezpieczone zostały za pomocą systemu monitoringu.	
9.	Pomieszczenia, w których przetwarzane są dane osobowe zabezpieczone zostały za pomocą nadzoru służby ochrony podczas nieobecności pracowników.	
10.	Pomieszczenia, w których przetwarzane są dane osobowe zabezpieczone zostały za pomocą nadzoru służby ochrony.	Całodobowo / Na czas nieobecności osób upoważnionych
11.	Dane osobowe w formie papierowej przechowywane są na otwartych regałach.	
12.	Dane osobowe w formie papierowej przechowywane są w zamkniętej niemetalowej szafie.	

13.	Dane osobowe w formie papierowej przechowywane są w zamkniętej metalowej szafie.	
14.	Dane osobowe w formie papierowej przechowywane są w zamkniętym sejfie lub kasie pancernej.	
15.	Kopie zapasowe / archiwalne danych osobowych przechowywane są w zamkniętej niemetalowej szafie.	
16.	Kopie zapasowe / archiwalne danych osobowych przechowywane są w zamkniętej metalowej szafie.	
17.	Kopie zapasowe/archiwalne danych osobowych przechowywane są w zamkniętym sejfie lub kasie pancernej.	
18.	Dane osobowe przetwarzane są w kancelarii tajnej, prowadzonej zgodnie z wymogami określonymi w odrębnych przepisach.	
19.	Pomieszczenia, w którym przetwarzane są dane osobowe zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy.	
20.	Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.	
21.	Komputery mobilne, na których przetwarzane są dane osobowe zabezpiecza się za pomocą kabli zabezpieczających.	
22.	Komputery mobilne, na których przetwarzane są dane osobowe zabezpiecza się za pomocą szafek zabezpieczających.	
23.	Monitory komputerów ustawione zostały w sposób uniemożliwiający wgląd osobom nieupoważnionym.	
24.	Monitory komputerów zabezpiecza się za pomocą filtrów prywatyzujących.	

Załącznik nr 13 – Ogólny opis technicznych środków bezpieczeństwa [WYPEŁNIA ASI]

ŚRODKI TECHNICZNE		
LP.	**Stosowane środki techniczne**	**Uwagi**
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		

Załącznik nr 14 – Wzory wyznaczenia oraz odwołania Oficera Bezpieczeństwa Danych Osobowych

Wyznaczenie Oficera Bezpieczeństwa Danych Osobowych

Niniejszym, reprezentując Administratora Danych - **Międzynarodowe Stowarzyszenie Studentów Medycyny IFMSA-Poland** z siedzibą w Warszawie, ul.Oczki 1A, 02-007 Warszawa, z dniem …/…/……,

wyznaczam

Panią / Pana …….

do pełnienia funkcji **Oficera Bezpieczeństwa Danych Osobowych (OBDO)** w **Międzynarodowe Stowarzyszenie Studentów Medycyny IFMSA-Poland**.

Upoważniam Panią / Pana ……. do przetwarzania danych osobowych we wszystkich zbiorach Administratora Danych w zakresie niezbędnym dla należytego wykonywania funkcji Oficera Bezpieczeństwa Danych Osobowych.

Zakres pozostałych obowiązków oraz warunki pełnienia funkcji Oficera Bezpieczeństwa Danych Osobowych określone zostały w Polityce ochrony danych osobowych wdrożonej w Międzynarodowe Stowarzyszenie Studentów Medycyny IFMSA-Poland.

Data i podpis osoby wyznaczanej do pełnienia funkcji OBDC	Data i podpis Administratora Danych

Odwołanie Oficera Bezpieczeństwa Danych Osobowych

Niniejszym, reprezentując Administratora Danych - **Międzynarodowe Stowarzyszenie Studentów Medycyny IFMSA-Poland** z siedzibą w Warszawie, ul.Oczki 1A, 02-007 Warszawa, z dniem …/…/……,

odwołuję

Panią / Pana …….

z pełnienia funkcji **Oficera Bezpieczeństwa Danych Osobowych (OBDO)** w **Międzynarodowe Stowarzyszenie Studentów Medycyny IFMSA-Poland**.

Data i podpis osoby odwoływanej z pełnienia funkcji OBDO

Data i podpis Administratora Danych

Wyznaczenie Administratora Systemów Informatycznych

Niniejszym, reprezentując Administratora Danych - **Międzynarodowe Stowarzyszenie Studentów Medycyny IFMSA-Poland** z siedzibą w Warszawie, ul. Oczki 1A, 02-007 Warszawa, z dniem …/…/…...,

wyznaczam

Panią / Pana …….

do pełnienia funkcji **Administratora Systemów Informatycznych (ASI)** w **Międzynarodowe Stowarzyszenie Studentów Medycyny IFMSA-Poland**.

Zakres obowiązków oraz warunki pełnienia funkcji Administratora Systemów Informatycznych określone zostały w Polityce ochrony danych osobowych wdrożonej w **Międzynarodowe Stowarzyszenie Studentów Medycyny IFMSA-Poland**.

Data i podpis osoby wyznaczanej do pełnienia funkcji ASI	Data i podpis Administratora Danych

Odwołanie Administratora Systemów Informatycznych

Niniejszym, reprezentując Administratora Danych - **Międzynarodowe Stowarzyszenie Studentów Medycyny IFMSA-Poland** z siedzibą w Warszawie, ul. Oczki 1A, 02-007 Warszawa, z dniem …/…/……,

odwołuję

Panią / Pana …….

z pełnienia funkcji **Administratora Systemów Informatycznych (ASI)** w **Międzynarodowe Stowarzyszenie Studentów Medycyny IFMSA-Poland**.

.

Data i podpis osoby odwoływanej z pełnienia funkcji ASI

Data i podpis Administratora Danych