Załącznik nr 1
do zarządzenia nr 24/2020
Rektora PMWSZ w Opolu
z dnia 24 kwietnia 2020 r.

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH DLA

PAŃSTWOWEJ MEDYCZNEJ WYŻSZEJ SZKOLE ZAWODOWEJ W OPOLU
UL. KATOWICKA 68, 45-060 OPOLE
NIP: 7542744054, REGON: 531304789

Pieczęć firmowa:	Podpis Administratora Danych osobowych:	Data podpisu ADO:

LISTA WYDAŃ.

Nr wyd.	Data	Opis zmian
1		Wydanie pierwsze

Spis treści

§ 1. WSTĘP

Realizując postanowienia 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) oraz wydane w oparciu o delegacje ustawą w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informacyjne służące do przetwarzania danych osobowych wprowadza się zestaw reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji informacji wrażliwej pozwalający na zapewnienie ochrony danych osobowych.

Celem Polityki Bezpieczeństwa jest zapewnienie ochrony danych osobowych przed wszelakiego rodzaju zagrożeniami, tak wewnętrznymi jak i zewnętrznymi, świadomymi lub nieświadomymi.

Jako Załącznik do niniejszej Polityki opracowano i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwaną dalej „Instrukcją zarządzania systemem informatycznym ”. Określa ona sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem zapewnienia ich bezpieczeństwa.

Ochrona danych osobowych jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez samych użytkowników.

Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić danym osobowym, że będą:

a. przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”);
b. zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze Przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami („ograniczenie celu”);
c. adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”);
d. prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość”);
e. przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie

środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania");

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

ADO jest odpowiedzialny za przestrzeganie w/w przepisów i musi być w stanie wykazać ich przestrzeganie („rozliczalność").

Polityka Bezpieczeństwa i Instrukcja zarządzania systemem informatycznym są dokumentami wewnętrznymi i nie mogą być udostępniane podmiotom trzecim bez uprzedniej zgody ADO.

§ 2. DEFINICJE

Przez użyte w Polityce określenia należy rozumieć:

1. **Polityka** – rozumie się przez to Politykę Bezpieczeństwa Ochrony Danych Osobowych.
2. **Administrator (zwany dalej jako Administrator Danych Osobowych (ADO)** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;
3. **Inspektor Ochrony Danych (IOD**) – Zgodnie z art. 37, 38, 39 RODO
4. **RODO** – rozumie się przez to ROZPORZĄDZENIAEPARLAMENTU 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).
5. **„Administrator Systemu Informatycznego"** (ASI) - osoba nadzorująca pracę systemu informatycznego oraz wykonująca w nim czynności wymagające specjalnych uprawnień
6. **„baza danych osobowych"** - zbiór uporządkowanych powiązanych ze sobą tematycznie zapisanych danych. Baza danych jest złożona z elementów o określonej strukturze - rekordów lub obiektów, w których są zapisane dane osobowe;
7. **„dane osobowe"** oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą") zwanej podmiotem danych; możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

8. **„dane genetyczne”** oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;
9. **„dane biometryczne”** oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;
10. **„dane dotyczące zdrowia”** oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia;
11. **„główna jednostka organizacyjna”** oznacza:
    a. jeżeli chodzi o ADO posiadającego jednostki organizacyjne w więcej niż jednym państwie członkowskim – miejsce, w którym znajduje się jego centralna administracja w Unii, a jeżeli decyzje co do celów i sposobów przetwarzania danych osobowych zapadają w innej jednostce organizacyjnej tego ADO w Unii i ta jednostka organizacyjna ma prawo nakazać wykonanie takich decyzji, to za główną jednostkę organizacyjną uznaje się jednostkę organizacyjną, w której zapadają takie decyzje;
    b. jeżeli chodzi o podmiot przetwarzający posiadający jednostki organizacyjne w więcej niż jednym państwie członkowskim – miejsce, w którym znajduje się jego centralna administracja w Unii lub, w przypadku gdy podmiot przetwarzający nie ma centralnej administracji w Unii – jednostkę organizacyjną podmiotu przetwarzającego w Unii, w której odbywają się główne czynności przetwarzania w ramach działalności jednostki organizacyjnej podmiotu przetwarzającego, w zakresie w jakim podmiot przetwarzający podlega szczególnym obowiązkom na mocy niniejszego RODO;
12. **„grupa przedsiębiorstw”** oznacza przedsiębiorstwo sprawujące kontrolę oraz przedsiębiorstwa przez nie kontrolowane;
13. **„Komisja”** – rozumie się przez to Komisję Europejską;
14. **„mający znaczenie dla sprawy i uzasadniony sprzeciw”** oznacza sprzeciw wobec projektu decyzji dotyczącej tego, czy doszło do naruszenia RODO lub czy planowane działanie wobec ADO lub podmiotu przetwarzającego jest zgodne z RODO, który to sprzeciw musi jasno wskazywać wagę wynikającego z projektu decyzji ryzyka naruszenia podstawowych praw lub wolności osób, których dane dotyczą, oraz gdy ma to zastosowanie – wagę ryzyka zakłócenia swobodnego przepływu danych osobowych w Unii;
15. **„naruszenie ochrony danych osobowych”** oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
16. **„nośnik komputerowy (wymienny)”** – nośnik służący do zapisu i przechowywania informacji np. CD, dyskietki, dyski twarde, pendrive, smartfony, dysk zewnętrzny.
17. **„odbiorca”** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą

otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; Przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;

18. **„organ nadzorczy”** oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51 RODO;
19. **„organ nadzorczy, którego sprawa dotyczy**” oznacza organ nadzorczy, którego dotyczy przetwarzanie danych osobowych, ponieważ: a) administrator lub podmiot przetwarzający posiadają jednostkę organizacyjną na terytorium państwa członkowskiego tego organu nadzorczego; b) przetwarzanie znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, mające miejsce zamieszkania w państwie członkowskim tego organu nadzorczego; lub c) wniesiono do niego skargę;
20. **„ograniczenie przetwarzania**” oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
21. **„organizacja międzynarodowa”** oznacza organizację i organy jej podlegające działające na podstawie prawa międzynarodowego publicznego lub inny organ powołany w drodze umowy między co najmniej dwoma państwami lub na podstawie takiej umowy;
22. **„podmiot przetwarzający”** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu ADO – zwany Procesorem;
23. **„profilowanie”** oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
24. **„przedstawiciel”** oznacza osobę fizyczną lub prawną mającą miejsce zamieszkania lub siedzibę w Unii, która została wyznaczona na piśmie przez ADO lub podmiot przetwarzający na mocy art. 27 RODO do reprezentowania ADO lub podmiotu przetwarzającego w zakresie ich obowiązków wynikających z RODO;
25. **„przedsiębiorca**” oznacza osobę fizyczną lub prawną prowadzącą działalność gospodarczą, niezależnie od formy prawnej, w tym spółki osobowe lub zrzeszenia prowadzące regularną działalność gospodarczą;
26. **„przetwarzanie”** oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
27. **„pseudonimizacja”** oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

28. **„system informatyczny" (system**) – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
29. **„strona trzecia"** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administratora, podmiot przetwarzający czy osoby, które – z upoważnienia ADO lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;
30. **„transgraniczne przetwarzanie"** oznacza:
    a. Przetwarzanie danych osobowych, które odbywa się w Unii w ramach działalności jednostek organizacyjnych w więcej, niż jednym państwie członkowskim ADO lub podmiotu przetwarzającego w Unii posiadającego jednostki organizacyjne w więcej niż jednym państwie członkowskim; albo
    b. Przetwarzanie danych osobowych, które odbywa się w Unii w ramach działalności pojedynczej jednostki organizacyjnej ADO lub podmiotu przetwarzającego w Unii, ale które znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, w więcej niż jednym państwie członkowskim;
31. **„usługa społeczeństwa informacyjnego"** oznacza usługę w rozumieniu art. 1 ust. 1 lit. b dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/1535 (1);
32. **„Użytkownik"** – pracownik posiadający uprawnienia do pracy w systemie informatycznym zgodnie ze swoim zakresem obowiązków;
33. **„wiążące reguły korporacyjne"** oznaczają Polityki ochrony danych osobowych stosowane przez ADO lub podmiot przetwarzający, którzy posiadają jednostkę organizacyjną na terytorium państwa członkowskiego, przy jednorazowym lub wielokrotnym przekazaniu danych osobowych administratorowi lub podmiotowi przetwarzającemu w co najmniej jednym państwie trzecim w ramach grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą;
34. **„zabezpieczenie systemu informatycznego**" – należy przez to rozumieć wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą;
35. **„zbiór danych"** oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
36. **„zgoda"** osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na Przetwarzanie dotyczących jej danych osobowych;
37. **„Zespół IT"** - komórka organizacyjna odpowiadająca za funkcjonowanie obszaru IT w przedsiębiorstwie.

USZCZEGÓŁOWIENIA

1. Państwowa Medyczna Wyższa Szkoła Zawodowa w Opolu, zwana dalej „ADO", utworzona została na podstawie rozporządzenia Rady Ministrów z dnia 8 kwietnia 2003 r. (Dz. U. Nr 64, poz. 593).
2. Uczelnia działa na podstawie ustawy z dnia 20 lipca 2018 r.– Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2018 r. poz.1668) , przepisów wydanych na jej podstawie oraz statutu.
3. Uczelnia posiada osobowość prawną.
   Nadzór nad Uczelnią sprawuje minister właściwy do spraw szkolnictwa wyższego.

4.. Za nadzór i monitorowanie przestrzegania Polityki odpowiadają:
   a. inspektor ochrony danych wyznaczony przez ADO w osobie Bożeny Krawczuk
5.. ADO przetwarza dane osobowe w sposób tradycyjny (papierowy) oraz w sposób częściowo zautomatyzowany tj. przy użyciu systemów informatycznych, w tym z wykorzystaniem usług chmurowych, zarówno w systemach zintegrowanych, jak i w rozproszonych zestawieniach.

§ 3. ZASADY PRZETWARZANIA

1. Przestrzegając zasad dotyczących przetwarzania danych osobowych, ADO zapewnia, by dane były:
   a. przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą ("zgodność z prawem, rzetelność i przejrzystość"),
   b. zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami ("ograniczenie celu");
   c. adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane ("minimalizacja danych");
   d. prawidłowe i w razie potrzeby uaktualniane; ADO podejmuje wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane ("prawidłowość");
   e. przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; ("ograniczenie przechowywania");
   f. przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych ("integralność i poufność").

2. Przetwarzanie danych osobowych możliwe jest w przypadku spełnienia jednej z przesłanek określonych w art. 6 ust. 1 lit. a-f Rozporządzenia, tj. w przypadku, gdy:

a. osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
b. przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
c. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na ADO;
d. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
e. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
f. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez ADO lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

3. Przetwarzanie szczególnych kategorii danych osobowych jest zabronione, chyba że spełniony jest jeden z warunków określonych w art. 9 ust. 1 lit. a-f RODO, tj. w przypadku, gdy:
   a. osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa powyżej;
   b. przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez ADO lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;
   c. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;
   d. przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;
   e. przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;
   f. przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;
   g. przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do

wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;

h. przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem odpowiednich warunków i zabezpieczeń;
i. przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową;
j. przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 RODO, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;
k. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez ADO lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

4. ADO na żądanie współpracuje z Organem nadzorczym w ramach wykonywania przez niego swoich zadań, w szczególności na jego żądanie udostępnia mu rejestr czynności przetwarzania w celu monitorowania operacji przetwarzania.
5. Za współpracę z Organem nadzorczym odpowiedzialny jest IOD (jeżeli został wyznaczony przez ADO do zapewnienia zgodności przetwarzania danych osobowych z przepisami prawa).
6. ADO śledzi wytyczne, zalecenia oraz najlepsze praktyki określone przez Europejską Radę Ochrony Danych na podstawie art. 70 ust. 1 lit. d-j i m RODO i uwzględnia je w swoich działaniach związanych z przetwarzaniem danych.

§ 4. ADMINISTRATOR DANYCH OSOBOWYCH

1. Do najważniejszych obowiązków ADO należy:
    1. uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, wdrażanie odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie

z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane,

2. stosowanie zatwierdzonych kodeksów postępowania, o których mowa w art. 40, lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42 RODO, może być wykorzystane jako element dla stwierdzenia przestrzegania przez ADO ciążących na nim obowiązków,
3. organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami RODO,
4. zapewnienie przetwarzania danych zgodnie z uregulowaniami niniejszej Polityki Bezpieczeństwa,
5. nadawanie upoważnień do przetwarzania danych osobowych dla osób przetwarzających te dane (Załącznik nr 2.2),
6. prowadzenie „Ewidencji osób upoważnionych do przetwarzania danych osobowych" (Załącznik nr 3),
7. prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych,
8. nadzór nad bezpieczeństwem danych osobowych,
9. kontrola działań poszczególnych osób oraz komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych oraz niniejszą dokumentacją,
10. kontrola przesłanek legalności przetwarzania danych osobowych zwykłych i wrażliwych,
11. dokonywanie anonimizacji danych w celu ochrony interesów osób, których dane dotyczą, a w szczególności celem zapewnienia, aby dane te były merytorycznie poprawne, prawidłowe, rzetelne i minimalne w stosunku do celów, w jakich są przetwarzane (Załącznik nr 20),
12. inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych,
13. aby zapewnić przetwarzanie danych zgodnie z zasadą integralności, rozliczalności, poufności, przejrzystości, zgodnie z prawem, z zapewnieniem minimalizacji danych i ich ograniczeniu przetwarzania, ADO prowadzi analizę wszystkich procesów przetwarzania zgodnie z Załącznikiem nr 25,
14. prowadzenie rejestru realizacji żądań podmiotu danych (Załącznik nr 17).

2. Prawa ADO.

ADO ma prawo do :

1. wyznaczania, rekomendowania i egzekwowania wykonania zadań związanych z ochroną danych osobowych w całej organizacji,
2. wstępu do pomieszczeń, w których zlokalizowane są zbiory danych i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z RODO oraz niniejszą dokumentacją,
3. żądania złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego,
4. żądania okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli,

5. żądać udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych.

3. Przetwarzanie danych osobowych przez ADO.
   1. ADO przetwarza dane osobowe zgodnie z prawem spełniając warunki:
      a. osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
      b. przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
      c. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na ADO;
      d. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
      e. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
      f. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez ADO lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

      Akapit pierwszy lit. f nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań.
   2. Aby spełnić zgodność przetwarzania danych zgodnie z prawem ADO prowadzi: analizę procesów przetwarzania (Załącznik nr 25), procedurę pozyskania zgody (Załącznik nr 26).

§ 5. WYZNACZANIE INSPEKTORA OCHRONY DANYCH

1. ADO wyznacza IOD, zawsze gdy:
   a. przetwarzania dokonuje organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;
      lub
   b. główna działalność ADO lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę;
      lub
   c. główna działalność ADO lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 RODO, oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10 RODO.
2. Analizę wyznaczenia IOD stanowi Załącznik nr 1.1.

3. IOD jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39 RODO. Załącznik nr 1 stanowi wzór wyznaczenia IOD.
4. ADO oraz podmiot przetwarzający wspierają IOD w wypełnianiu przez niego zadań, o których mowa w art. 39 RODO, 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.
5. ADO oraz podmiot przetwarzający zapewniają, by IOD nie otrzymywał instrukcji dotyczących wykonywania tych zadań. Nie jest on odwoływany ani karany przez ADO ani podmiot przetwarzający za wypełnianie swoich zadań. IOD bezpośrednio podlega najwyższemu kierownictwu ADO lub podmiotu przetwarzającego.
6. ADO oraz podmiot przetwarzający zapewniają, by IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.
7. IOD jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań – zgodnie z prawem Unii lub prawem państwa członkowskiego.

§ 6. ZASADY DOPUSZCZANIA OSÓB WEWNĄTRZ ORGANIZACJI DO PRZETWARZANIA DANYCH

1. Do przetwarzania danych osobowych mogą zostać dopuszczone wyłącznie osoby przeszkolone, którym ADO nadał na piśmie lub w formie dokumentowej odpowiednie upoważnienie do przetwarzania danych osobowych – wzór upoważnienia do przetwarzania danych osobowych stanowi Załącznik nr 2.2.
2. Z zastrzeżeniem ust. 3 niniejszego paragrafu, każdy dopuszczony do przetwarzania danych osobowych pracownik po odbyciu szkolenia oraz po otrzymaniu upoważnienia do przetwarzania danych osobowych składa na piśmie oświadczenie o poufności, którego treść uzależniona jest od zakresu obowiązków danego pracownika– wzór oświadczenia o poufności stanowi Załącznik nr 2.1.
3. W przypadku, gdy do przetwarzania danych osobowych dopuszczona jest osoba świadcząca pracę w ramach cywilnoprawnej formy zatrudnienia lub osoba prowadząca indywidualną działalność gospodarczą, stale współpracująca z ADO, od osoby takiej, po nadaniu jej na piśmie lub w formie dokumentowej odpowiedniego upoważnienia do przetwarzania danych osobowych, odbiera się oświadczenie o poufności będące Załącznikiem nr 2.1.
4. W przypadku, gdy podmiot zewnętrzny deleguje swoich pracowników lub osoby świadczące u niego pracę w ramach cywilnoprawnych form zatrudnienia do świadczenia usług pod kontrolą i na fizycznym obszarze przetwarzania danych ADO oraz jeżeli nie zachodzi relacja uzasadniająca zawarcie umowy powierzenia, wyżej wymienionym pracownikom lub osobom nadawane jest na piśmie lub w formie dokumentowej upoważnienie do przetwarzania danych osobowych i odbierane jest od nich pisemne oświadczenie o poufności – wzór oświadczenia o poufności stanowi Załącznik nr 2.1.
5. ADO zapewnia, by każda osoba fizyczna działająca z jego upoważnienia, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie ADO, chyba że wymaga tego od niej prawo Unii lub prawo państwa członkowskiego.

6. Upoważnienie, o którym mowa w ustępie 1 powyżej, musi być aktualne. W przypadku przedłużającej się nieobecności osoby upoważnionej lub zaprzestania wykonywania przez nią części lub wszystkich obowiązków, uzasadniających potrzebę upoważnienia jej do przetwarzania danych osobowych, upoważnienie musi zostać w odpowiednim zakresie odwołane.
7. Utrata uprawnień do przetwarzania danych osobowych objętych upoważnieniem może nastąpić w szczególności w przypadku:
    1. odwołania upoważnienia przez ADO bez podania przyczyny;
    2. rozwiązania stosunku pracy bądź innego stosunku prawnego łączącego osobę upoważnioną z ADO;
    3. zmiany stanowiska pracy osoby upoważnionej u ADO na stanowisko nieuzasadniające konieczności posiadania dostępu do zbiorów danych osobowych, jeżeli nowy zakres czynności nie wykazuje obowiązków służbowych związanych z przetwarzaniem danych osobowych;
    4. umyślnego naruszenia przez osobę upoważnioną zasad ochrony danych osobowych określonych w RODO, Polityce Bezpieczeństwa.
8. W przypadku utraty uprawnień do przetwarzania danych osobowych, ADO niezwłocznie odwołuje upoważnienie do przetwarzania danych osobowych oraz dokonuje zmian w ewidencji osób upoważnionych do przetwarzania danych osobowych.
9. ADO prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych w wersji papierowej/elektronicznej odnotowując informacje o wszystkich wydanych upoważnieniach oraz adnotacje o ich odwołaniu – wzór ewidencji osób upoważnionych stanowi Załącznik nr 3 do Polityki.
10. Dla wszystkich Użytkowników stosowane są uprawnienia do zasobów i zbiorów wedle zasady niezbędnego minimum potrzebnego do wykonywania obowiązków pracowniczych lub służbowych.
    1. Gdy nie zostanie powołany ASI jego obowiązki spełnia ADO lub osoba przez niego powołana.
    2. ASI nadaje, zmienia lub odwołuje uprawnienia w systemie informatycznym zgodnie z dyspozycjami ADO zgodnie z Załącznikiem nr 19.1.
    3. Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych, mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie do przetwarzania danych osobowych nadane przez ADO
    4. Użytkownicy powinni pracować na kontach zwykłych Użytkowników. Praca na kontach administracyjnych jest dopuszczalna tylko dla ASI oraz upoważnionych przez niego osób.
    5. W przypadku wycofania uprawnień Użytkownika do systemu informatycznego, w którym przetwarzane są dane osobowe, ASI niezwłocznie blokuje konto Użytkownika i informuje o tym fakcie ADO i IOD.
    6. Identyfikator nowego konta w systemie informatycznym nadany zgodnie z wnioskiem przez ASI musi być unikalny w obrębie systemu.
    7. Za kontrolę aktualności kont Użytkowników wraz z uprawnieniami im nadanymi odpowiedzialny jest ASI.
    8. Osobą zastępującą ASI w sytuacjach awaryjnych jest pracownik działu IT wskazany przez ASI.
11. Każdy pracownik przed nadaniem mu upoważnienia do przetwarzania danych osobowych zostaje przeszkolony z zakresu ochrony danych osobowych przez IOD/ osobę wyznaczoną przez ADO, przy czym szkolenie to zostaje zakończone podpisaniem przez osobę szkoloną oświadczenia o wzięciu

udziału w szkoleniu oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych.

12. W przypadku zmian przepisów dotyczących ochrony danych osobowych lub zasad przetwarzania i ochrony danych osobowych u ADO, IOD/ osoba wyznaczona przez ADO niezwłocznie organizuje szkolenie dla pracowników.
13. Tematyka szkoleń dotyczy w szczególności:
    a. treści przepisów dotyczących ochrony danych osobowych;
    b. sporządzania i przechowywania sporządzania kopii zapasowych, niszczenia wydruków i zapisów na nośnikach;
    c. sposobów ochrony danych osobowych przed osobami postronnymi;
    d. procedur udostępniania danych osobom;
    e. praw osób, których dane dotyczą;
    f. obowiązków osób upoważnionych do przetwarzania danych osobowych;
    g. zasad przetwarzania i ochrony danych osobowych określonych w Polityce.
14. W celu przeprowadzenia szkolenia IOD osoba wyznaczona przez ADO może korzystać z pomocy wyspecjalizowanych podmiotów zewnętrznych posiadających odpowiednio wysoki poziom wiedzy i kwalifikacje do prowadzenia szkoleń z zakresu ochrony danych osobowych.
15. IOD/ osoba wyznaczona przez ADO prowadzi dokumentację dotyczącą przeprowadzonych szkoleń, w tym sporządza po przeprowadzeniu każdego szkolenia listę osób, które wzięły w nim udział.

§ 7. POWIERZENIE PRZETWARZANIA DANYCH

ADO powierza przetwarzanie danych podmiotom przetwarzającym zgodnie z poniższymi zasadami:

1. Jeżeli przetwarzanie ma być dokonywane w imieniu ADO, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.
2. Podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody ADO. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje ADO o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.

   Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy (wzór umowy stanowi Załącznik nr 14) lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i ADO, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa ADO. Ta umowa lub inny instrument prawny stanowią w szczególności, że podmiot przetwarzający:

   a. przetwarza dane osobowe wyłącznie na udokumentowane polecenie ADO – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej –

chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje ADO o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;

b. zapewnia, że osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub podlegają odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
c. podejmuje wszelkie środki wymagane na mocy art. 32 RODO;
d. przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, o których mowa w ust. 2 i 4;
e. biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga ADO poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III RODO;
f. uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36 RODO;
g. po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji ADO usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;
h. udostępnia ADO wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwia administratorowi lub audytorowi upoważnionemu przez ADO przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

3. Jeżeli do wykonania w imieniu ADO konkretnych czynności przetwarzania podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający nałożone zostają – na mocy umowy lub innego aktu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego – te same obowiązki ochrony danych jak w umowie lub innym akcie prawnym między administratorem a podmiotem przetwarzającym, o których to obowiązkach mowa w ust. 3, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom niniejszego rozporządzenia. Jeżeli ten inny podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec ADO za wypełnienie obowiązków tego innego podmiotu przetwarzającego spoczywa na pierwotnym podmiocie przetwarzającym.
4. Wystarczające gwarancje, o których mowa w ust. 1 i 4 niniejszego paragrafu, podmiot przetwarzający może wykazać między innymi poprzez stosowanie zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 RODO lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42 RODO.
5. ADO w celu spełnienia gwarancji, o których mowa w ust.1 i 4 niniejszego paragrafu, każdorazowo bada podmiot przetwarzający zgodnie z Załącznikiem 13.1.
6. Bez uszczerbku dla indywidualnych umów między ADO a podmiotem przetwarzającym, umowa lub inny akt prawny, o których mowa w ust. 3 i 4 niniejszego paragrafu, mogą się opierać w całości lub w części na standardowych klauzulach umownych, o których mowa w ust. 7 i 8 niniejszego paragrafu,

także gdy są one elementem certyfikacji udzielonej ADO lub podmiotowi przetwarzającemu zgodnie z art. 42 i 43 RODO.

7. ADO w miarę potrzeby przeprowadzi audyt podmiotu przetwarzającego w zakresie zgodności wykonywania przez niego czynności przetwarzania danych osobowych z postanowieniami umowy oraz obowiązującymi przepisami o ochronie danych, w szczególności w celu sprawdzenia wykonywania przez podmiot przetwarzający ciążących na nim obowiązków.
8. Zasady przeprowadzenia audytu określa umowa, o której mowa w ust.12. niniejszego paragrafu.
9. ADO przekaże podmiotowi przetwarzającemu, po przeprowadzonym audycie, pisemne zalecenia i wytyczne wraz z terminem ich realizacji, dotyczące w szczególności zabezpieczenia danych osobowych pod względem technicznym i organizacyjnym oraz sposobu wykonywania czynności ich przetwarzania.
10. ADO może zrezygnować z przeprowadzenia audytu podmiotu przetwarzającego jedynie w wyjątkowych przypadkach, gdy powierzenie przetwarzania ma charakter bagatelny.
11. Umowa lub inny akt prawny, o których mowa w ust. 3 i 4, mają formę pisemną także formę elektroniczną zgodnie z Załącznikiem nr 14.
12. Umowa, na podstawie której odbywa się przetwarzanie danych, powinna określać:
    - przedmiot przetwarzania,
    - czas trwania przetwarzania,
    - charakter przetwarzania,
    - cel przetwarzania,
    - rodzaj powierzonych danych osobowych,
    - kategorie osób, których dane dotyczą,
    - obowiązki i prawa ADO,
    - obowiązki Procesora, w tym dotyczące przeprowadzania audytu przez ADO,
    - warunki dalszego powierzenia przetwarzania danych, w szczególności wskazanie, czy wymaga ono szczegółowej, czy ogólnej pisemnej zgody ADO.
13. Wzór umowy powierzenia przetwarzania danych osobowych oraz wzór postanowień regulujących Powierzenie przetwarzania danych osobowych, niestanowiących odrębnej umowy, ale sformułowanych w celu uzupełnienia innych zawieranych umów, stanowią Załączniki do Polityki.
14. ADO odnotowuje w rejestrze czynności przetwarzania umowy powierzenia przetwarzania.
15. Bez uszczerbku dla art. 82, 83 i 84 RODO, jeżeli podmiot przetwarzający naruszy niniejsze rozporządzenie przy określaniu celów i sposobów przetwarzania, uznaje się go za ADO w odniesieniu do tego przetwarzania.
16. Podmiot przetwarzający oraz każda osoba działająca z upoważnienia ADO lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie ADO, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego.
17. ADO prowadzi Rejestr powierzeń podmiotom zewnętrznym zgodnie z Załącznikiem nr 13.
18. ADO jako podmiot przetwarzający oraz – gdy ma to zastosowanie – przedstawiciel podmiotu przetwarzającego prowadzą rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu ADO będący Załącznikiem nr 13.2.

§ 8. ZASADY UJAWNIANIA DANYCH OSOBOWYCH ODBIORCOM INNYM NIŻ PROCESOR

1. Ujawnianie danych osobowych odbiorcom innym niż Procesor dopuszczalne jest tylko w przypadku spełnienia jednej z przesłanek przetwarzania danych osobowych określonych w § 2 Polityki.
2. Ujawnianie danych osobowych może nastąpić tylko po uprzednim przedstawieniu wniosku (zgodnie z Załącznikiem nr 12.1) o ich ujawnienie. Wniosek powinien mieć formę pisemną lub dokumentową i zawierać:
   a. oznaczenie wnioskodawcy;
   b. wskazanie podstaw legalizacyjnych uzasadniających żądanie ujawnienia;
   c. określenie rodzaju i zakresu żądanych informacji oraz formy ich przekazania lub udostępnienia;
   d. wskazanie imienia, nazwiska i stanowiska osoby upoważnionej do otrzymania danych osobowych lub zapoznania się z ich treścią.
3. Ujawnianie danych osobowych na podstawie ustnego wniosku zawierającego wszystkie cztery elementy określone w ust. 2 może nastąpić wyłącznie, gdy zachodzi konieczność niezwłocznego działania.
4. Osoba udostępniająca dane osobowe jest obowiązana zażądać od osoby uprawnionej określonej w ust. 2 pkt.d jako upoważniona pokwitowania ujawnienia danych, zawierającego informacje przekazane na podstawie wniosku złożonego na piśmie lub w formie dokumentowej albo potwierdzenie faktu uzyskania wglądu w treść informacji.
5. Jeśli informacje są przekazywane na podstawie ustnego wniosku, należy stosownie do okoliczności zwrócić się z prośbą o pokwitowanie albo potwierdzenie otrzymania informacji. Jeśli pokwitowanie albo potwierdzenie ze względu na okoliczności udostępniania nie są możliwe, osoba udostępniająca informacje sporządza na tę okoliczność notatkę służbową.
6. Jeśli osoba uprawniona pouczyła osobę udostępniającą informacje o konieczności zachowania w tajemnicy faktu i okoliczności przekazania informacji, to okoliczność ta jest odnotowywana w rejestrze czynności przetwarzania niezależnie od odnotowania faktu udostępnienia informacji.
7. W celu zapewnienia kontroli nad tym, jakie dane osobowe, kiedy i przez kogo oraz komu zostały przekazane, ADO odnotowuje ujawnienie danych w rejestrze czynności przetwarzania.
8. Ujawnianie danych osobowych podmiotom mającym siedzibę w jednym z państw Europejskiego Obszaru Gospodarczego podlega ogólnym zasadom przetwarzania danych osobowych wynikającym z RODO. ADO danych z EOG, tak samo jak ADO przetwarzający Dane na terytorium Polski, jest zobowiązany m.in. do wypełnienia jednego z warunków legalności przetwarzania Danych osobowych, przestrzegania zasad przetwarzania danych określonych w § 4 oraz do wdrożenia odpowiednich środków technicznych i organizacyjnych, zapewniających odpowiedni stopień bezpieczeństwa danych.

§ 9. TRANSFER DANYCH DO PAŃSTW TRZECICH

1. ADO przekazuje dane do państwa trzeciego lub organizacji międzynarodowej wyłącznie pod warunkiem spełnienia kryteriów określonych poniżej, dbając o to, by nie został naruszony stopień ochrony osób fizycznych zagwarantowany w RODO.
2. Przekazanie danych do państwa trzeciego lub organizacji międzynarodowej może nastąpić, jeżeli Komisja stwierdziła, że to Państwo trzecie, terytorium lub określone sektory w tym państwie trzecim lub dana Organizacja międzynarodowa zapewniają odpowiedni stopień ochrony;
3. W przypadku braku decyzji Komisji, o której mowa w ust. 2, przekazanie danych do państwa trzeciego może nastąpić, jeżeli:
    a. zostały zapewnione odpowiednie zabezpieczenia ochrony danych osobowych niewymagające uzyskania specjalnego zezwolenia ze strony organu nadzorczego, za pomocą jednego z następujących instrumentów:
        - prawnie wiążącego i egzekwowalnego instrumentu między organami lub podmiotami publicznymi;
        - wiążących reguł korporacyjnych, szczegółowo uregulowane w art. 47 RODO;
        - standardowych klauzul ochrony danych przyjętych przez Komisję zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 2 RODO;
        - standardowych klauzul ochrony danych przyjętych przez organ nadzorczy i zatwierdzonych przez Komisję zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 2 RODO;
        - zatwierdzonego kodeksu postępowania zgodnie z art. 40 RODO wraz z wiążącymi i egzekwowalnymi zobowiązaniami ADO lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich gwarancji, w tym w odniesieniu do praw osób, których dane dotyczą; lub
        - zatwierdzonego mechanizmu certyfikacji zgodnie z art. 42 RODO wraz z wiążącymi i egzekwowalnymi zobowiązaniami ADO lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich gwarancji, w tym w odniesieniu do praw osób, których dane dotyczą;
    b. zostały zapewnione odpowiednie zabezpieczenia ochrony danych osobowych za pomocą jednego z następujących instrumentów:
        - klauzul umownych między ADO lub Procesorem a ADO, Procesorem lub odbiorcą danych w państwie trzecim lub organizacji międzynarodowej; lub
        - postanowień porozumień administracyjnych między organami lub podmiotami publicznymi, w których przewidziano egzekwowalne i skuteczne prawa osób, których dane dotyczą - pod warunkiem uzyskania zezwolenia właściwego organu nadzorczego.
4. W przypadku braku decyzji Komisji, o której mowa w ust. 2, lub w przypadku braku odpowiednich zabezpieczeń, o których mowa w ust. 3, jednorazowe lub wielokrotne przekazanie danych osobowych do państwa trzeciego może nastąpić, wyłącznie pod warunkiem, że:

- osoba, której dane dotyczą, poinformowana o ewentualnym ryzyku, z którym - ze względu na brak decyzji stwierdzającej odpowiedni stopień ochrony oraz na brak odpowiednich zabezpieczeń - może się dla niej wiązać proponowane przekazanie, wyraźnie wyraziła na nie zgodę;
- przekazanie jest niezbędne do wykonania umowy między osobą, której dane dotyczą, a ADO lub do wprowadzenia w życie środków przed umownych podejmowanych na żądanie osoby, której dane dotyczą;
- przekazanie jest niezbędne do zawarcia lub wykonania umowy zawartej w interesie osoby, której dane dotyczą, między ADO a inną osobą fizyczną lub prawną;
- przekazanie jest niezbędne ze względu na ważne względy interesu publicznego;
- przekazanie jest niezbędne do ustalenia, dochodzenia lub ochrony roszczeń;
- przekazanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innych osób, jeżeli osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody; lub
- przekazanie następuje z rejestru, który zgodnie z prawem Unii lub prawem polskim ma służyć za źródło informacji dla ogółu obywateli i który jest dostępny dla ogółu obywateli lub dla każdej osoby mogącej wykazać prawnie uzasadniony interes - ale wyłącznie w zakresie, w jakim w danym przypadku spełnione zostały warunki takiego dostępu określone w prawie Unii lub w prawie polskim.

5. Przekazanie danych do państwa trzeciego lub organizacji międzynarodowej jest odnotowywane w rejestrze czynności przetwarzania wraz ze wskazaniem podstawy przekazania.

§ 10. ZAKOŃCZENIE PRZETWARZANIA – POLITYKA RETENCJI

1. Dane osobowe są przechowywane przez okres nie dłuższy niż jest to niezbędne do celów, w których dane te są przetwarzane. Okresy przechowywania poszczególnych kategorii danych osobowych określa Załącznik nr 23 do Polityki.
2. Po zakończeniu przetwarzania danych osobowych ADO zobowiązany jest do niezwłocznego usunięcia danych osobowych i wszelkich istniejących ich kopii, zarówno elektronicznych, jak i papierowych.
3. Z usunięcia danych osobowych i ich kopii ADO sporządza protokół.

§ 11. PRAWA PODMIOTU DANYCH

1. W celu realizacji swoich praw, podmiot danych kontaktuje się z IOD, jeżeli został on powołany. W innym wypadku podmiot danych powinien kontaktować się z ADO e-mail: biurorektora@wsm.opole.pl
2. Przetwarzanie danych osobowych przez ADO powinno być zgodne z prawem, rzetelne oraz przejrzyste dla osób, których dane dotyczą. Wszelkie informacje i wszelkie komunikaty związane z przetwarzaniem tych danych osobowych powinny być łatwo dostępne, zrozumiałe oraz sformułowane jasnym i prostym językiem. Zasada ta dotyczy w szczególności informowania osób, których dane dotyczą, o tożsamości ADO i celach przetwarzania oraz innych informacji mających zapewnić rzetelność

i przejrzystość przetwarzania w stosunku do osób, których sprawa dotyczy, a także prawa takich osób do uzyskania potwierdzenia i informacji o przetwarzanych danych osobowych ich dotyczących.

3. Osobom, których dane dotyczą, należy uświadamiać ryzyka, zasady, zabezpieczenia i prawa związane z przetwarzaniem danych osobowych oraz sposoby wykonywania praw przysługujących im w związku z takim przetwarzaniem. W szczególności konkretne cele przetwarzania danych osobowych przez ADO powinny być wyraźne, uzasadnione i określone w momencie ich zbierania.
4. Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, ADO podczas pozyskiwania danych osobowych podaje jej informacje określone w § 13 ust. 1, 2 i 3 RODO, chyba że ta osoba dysponuje już tymi informacjami.
5. Jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą, ADO podaje jej informacje określone w § 14 ust. 1, 2 i 4 RODO, chyba że:
    a. ta osoba dysponuje już tymi informacjami;
    b. udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku;
    c. pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega ADO, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą; lub
    d. dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy.
6. Informacje, o których mowa w ust. 2, ADO podaje:
    a. w rozsądnym terminie po pozyskaniu danych osobowych - najpóźniej w ciągu miesiąca - mając na uwadze konkretne okoliczności przetwarzania danych osobowych;
    b. jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą - najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą; lub
    c. jeżeli planuje się ujawnić dane osobowe innemu odbiorcy - najpóźniej przy ich pierwszym ujawnieniu.
7. Wzory klauzul informacyjnych stosowanych w przypadkach, o których mowa w ust. 1 i 2, stanowią Załączniki nr 16 do Polityki bezpieczeństwa.
8. Jeżeli podstawą przetwarzania danych osobowych jest zgoda osoby, której dane dotyczą, ADO musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych.
9. Zgoda powinna być dobrowolnym, konkretnym, świadomym i jednoznacznym okazaniem woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych w konkretnym celu. Na różne cele przetwarzania powinna być odbierana osobna zgoda.
10. Jeżeli osoba, której dane dotyczą, wyrażą zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Wzór zapytania o zgodę składanego w formie pisemnej/ elektronicznej/ telefonicznej/ przy osobistym kontakcie z osobą, której dane dotyczą, stanowi Załącznik nr 26 do Polityki Bezpieczeństwa.

11. ADO umożliwia osobie, której dane dotyczą, wycofanie zgody w dowolnym momencie w taki sam sposób, w jaki nastąpiło jej wyrażenie. ADO w jasny i przejrzysty sposób informuje osobę, której dane dotyczą, o możliwości wycofania zgody. W przypadku wycofania zgody ADO niezwłocznie zaprzestaje przetwarzania danych tej osoby.
12. Wyrażenie zgody na przetwarzanie danych nie może stanowić warunku zawarcia umowy lub świadczenia usługi.
13. W przypadku planu zmiany celu przetwarzania danych, ADO ponownie zwraca się do osoby, której dane dotyczą, o zgodę na przetwarzanie jej danych co do zmienianego celu.
14. ADO umożliwia osobie, której dane dotyczą, uzyskanie potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, również uzyskanie dostępu do nich i informacji określonych w § 15 ust. 1 i 2 RODO.
15. ADO dostarcza każdej zwracającej się do ADO osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, ADO pobiera opłatę w wysokości, która wynikają z kosztów administracyjnych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się w korespondencji mailowej.
16. ADO dokonuje sprostowania nieprawidłowych danych na żądanie osoby, której dane dotyczą, niezwłocznie po otrzymaniu takiego żądania.
17. ADO uzupełnia niekompletne dane osobowe na żądanie osoby, której dane dotyczą, niezwłocznie po otrzymaniu takiego żądania. ADO odmawia uzupełnienia danych osobowych, gdy jest ono niezgodne z celami przetwarzania.
18. ADO weryfikuje merytoryczną poprawność danych osobowych wskazanych w żądaniu sprostowania lub uzupełnienia danych.
19. ADO informuje o sprostowaniu każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. ADO informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.
20. Na żądanie osoby, której dane dotyczą, ADO usuwa dotyczące je dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:
    a. dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
    b. osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie, i nie ma innej podstawy prawnej przetwarzania;
    c. osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 RODO wobec przetwarzania;
    d. dane osobowe były przetwarzane niezgodnie z prawem;
    e. dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega ADO;
    f. dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego,
21. Jeżeli ADO upublicznił dane osobowe, które zgodnie z ust. 1 ma obowiązek usunąć, to - biorąc pod uwagę dostępną technologię i koszt realizacji - podejmuje rozsądne działania, w tym środki techniczne,

by poinformować Administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by Administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje. ADO informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

22. ADO może odmówić usunięcia danych w zakresie, w jakim jest ono niezbędne:
    a. do korzystania z prawa do wolności wypowiedzi i informacji;
    b. do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega ADO, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej ADO;
    c. z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h oraz i art. 9 ust. 3 RODO;
    d. do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 RODO, o ile prawdopodobne jest, że usunięcie danych uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub
    e. do ustalenia, dochodzenia lub obrony roszczeń.
23. ADO zaniecha przetwarzania danych osobowych niezwłocznie po otrzymaniu sprzeciwu osoby, której dane dotyczą, jeżeli przetwarzanie było niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej ADO lub do celów wynikających z prawnie uzasadnionych interesów realizowanych przez ADO lub przez stronę trzecią. ADO może nie uwzględnić sprzeciwu, jeżeli wykaże istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.
24. ADO zaniecha przetwarzania danych osobowych do celów marketingu bezpośredniego niezwłocznie po otrzymaniu sprzeciwu osoby, której dane dotyczą, wobec przetwarzania do takich celów.
25. Osoba, której dane dotyczą, może żądać usunięcia danych lub złożyć sprzeciw w formie pisemnej, elektronicznej, w tym za pośrednictwem strony internetowej ADO, telefonicznie lub ustnie do protokołu w siedzibie ADO.
26. Jeżeli przetwarzanie odbywa się na podstawie zgody osoby, której dane dotyczą, i w sposób zautomatyzowany, ADO umożliwia osobom, których dane dotyczą, otrzymanie kopii ich danych osobowych w formie elektronicznej, w formacie *.xml, *.json, *.csv lub innym powszechnie używanym, ustrukturyzowanym formacie, nadającym się do odczytu maszynowego, umożliwiającym tej osobie przesłanie danych do innego dostawcy usług, odczytanie danych w sposób automatyczny przez innego dostawcę i korzystanie z danych w ramach usług innego dostawcy.
27. O ile jest to technicznie możliwe, na żądanie osoby, której dane dotyczą, ADO przesyła dane osobowe bezpośrednio innemu ADO.
28. ADO może odmówić udostępnienia kopii danych zgodnie z ust. 1, jeżeli mogłoby ono niekorzystnie wpływać na prawa i wolności innych.
29. ADO ogranicza przetwarzanie danych na żądanie osoby, której dane dotyczą, w następujących przypadkach:

a. osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych - na okres pozwalający ADO sprawdzić prawidłowość tych danych;
b. przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
c. ADO nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
d. osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania - do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie ADO są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

30. ADO przechowuje dane, których przetwarzanie zostało ograniczone zgodnie z ust. 29, a w pozostałym zakresie przetwarza je wyłącznie:
    a. za zgodą osoby, której dane dotyczą, lub
    b. w celu ustalenia, dochodzenia lub obrony roszczeń, lub
    c. w celu ochrony praw innej osoby fizycznej lub prawnej, lub
    d. z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.
31. Przed uchyleniem ograniczenia przetwarzania ADO informuje o tym osobę, której dane dotyczą, która żądała ograniczenia.
32. ADO informuje o ograniczeniu przetwarzania każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. ADO informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.
33. ADO dopuszcza podejmowanie decyzji, które opierają się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołują skutki prawne wobec osoby, której dane dotyczą, lub w podobny sposób istotnie na nią wpływają, wyłącznie jeżeli taka decyzja:
    a. jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a ADO;
    b. jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega ADO i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą; lub
    c. opiera się na wyraźnej zgodzie osoby, której dane dotyczą.
34. W przypadkach, o których mowa w ust.33 lit. a i c, na żądanie osoby, której dane dotyczą, ADO zapewni weryfikację interwencją ludzką. ADO umożliwi osobie, której dane dotyczą, wyrażenie własnego stanowiska i zakwestionowanie decyzji podjętej w sposób określony w ust.33
35. Decyzje, o których mowa w ust. 34, nie mogą opierać się na szczególnych kategoriach danych osobowych, chyba że zastosowanie ma art. 9 ust. 2 lit. a lub g RODO i istnieją właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą.
36. ADO wprowadza Regulamin zarzadzania skargami i wnioskami w związku z przetwarzaniem danych osobowych będący Załącznikiem nr 29.

§ 12. REJESTR CZYNNOŚCI PRZETWARZANIA

1. ADO niezależnie od zastosowania art. 30 ust. 5 RODO w celu zapewnienia przetwarzania zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą – prowadzi Rejestr czynności przetwarzania będący Załącznikiem nr 27. W rejestrze tym zamieszcza się wszystkie następujące informacje:
   a. imię i nazwisko lub nazwę oraz dane kontaktowe ADO oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela ADO oraz IOD;
   b. cele przetwarzania;
   c. opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
   d. kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
   e. gdy ma to zastosowanie, o przekazaniu 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;
   f. jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
   g. jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

§ 13. EWIDENCJA OBSZARÓW PRZETWARZANIA, ZBIORÓW DANYCH ORAZ OPROGRAMOWANIA

1. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w których przetwarzane są dane osobowe.
   Szczegółowe rozmieszczenie zbiorów dokumentacji papierowej i elektronicznej, zawierającej dane osobowe, opisane jest w Załączniku nr 4.
2. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.
   Wykaz zbiorów danych osobowych w postaci dokumentacji papierowej i elektronicznej wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, opisany jest w Załączniku nr 5.
3. Ewidencja systemów IT.
   Ewidencję systemów IT przedstawiono w Załączniku nr 6.

§ 14. ZABEZPIECZENIA, ŚRODKI ORGANIZACYJNE I TECHNICZNE NIEZBĘDNE DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

1. Zabezpieczenia organizacyjne zastosowane przez ADO:
   a. została opracowana i wdrożona Polityka Bezpieczeństwa;
   b. została opracowana i wdrożona instrukcja zarządzania systemem informatycznym;

c. do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające ważne upoważnienia nadane przez ADO;
d. prowadzona jest ewidencja osób upoważnionych do przetwarzania danych;
e. osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego;
f. osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy;
g. przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych;
h. przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych;
i. stosuje się pisemne umowy powierzenia przetwarzania danych dla współpracy z podwykonawcami przetwarzającymi dane osobowe.

2. Zabezpieczenia ochrony fizycznej danych osobowych.
   Zabezpieczenia fizyczne opisane są w Załączniku nr 5.
3. Zabezpieczenia sprzętowe infrastruktury informatycznej i telekomunikacyjnej.
   Zabezpieczenia stosuje się dla fizycznych elementów systemu, ich połączeń oraz systemów operacyjnych. Szczegółowy opis zabezpieczeń zawarty jest w instrukcji zarządzania systemem informatycznym.
4. Zabezpieczenia baz danych.
   Zabezpieczenia techniczne i programowe stosuje się dla procedur, aplikacji, programów i innych narzędzi programowych przetwarzających dane osobowe. Szczegółowy opis zabezpieczeń zawarty jest w Instrukcji zarządzania systemem informatycznym.

§ 15. REALIZACJA ZASADY PRIVACY BY DESIGN I PRIVACY BY DEFAULT

1. ADO w momencie ustalania sposobów przetwarzania danych, jak i w trakcie samego procesu przetwarzania, wdraża odpowiednie środki techniczne i organizacyjne, tak aby przetwarzanie było zgodne z wymogami RODO i efektywnie chroniło prawa osób, których dane dotyczą, przy uwzględnieniu charakteru, zakresu, kontekstu i celu przetwarzania danych oraz wynikającego z nich ryzyka dla praw i wolności osób fizycznych.
2. ADO wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, że domyślnie dane osobowe nie będą udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.

3. ADO dokumentuje ochronę danych osobowych w fazie projektowania, za pomocą listy kontrolnej podsumowującej fazę projektowania ze wskazaniem przeanalizowanych rozwiązań w zakresie ochrony danych osobowych.

§ 16. OCENA SKUTKÓW DLA OCHRONY DANYCH

1. Jeżeli na podstawie analizy ryzyka wynika, że dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, ADO przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. W celu określenia, czy dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, ADO weryfikuje:
    a. charakter,
    b. zakres,
    c. kontekst i
    d. cele przetwarzania.
2. Ocena skutków dla ochrony danych jest wymagana w szczególności w przypadku, gdy przetwarzanie spełnia dwa lub więcej z poniższych kryteriów:
    a. przetwarzanie wiąże się z oceną lub punktacją w tym profilowaniem i prognozowaniem 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;
    b. dochodzi do automatycznego podejmowania decyzji wywołującej wobec osoby, której dane dotyczą, skutki prawne lub w podobny sposób istotnie na nią wpływającej;
    c. przetwarzanie obejmuje szczególne kategorie danych osobowych lub danych o charakterze wysoce osobistym;
    d. dochodzi do przetwarzania danych na dużą skalę;
    e. przetwarzanie jest wykorzystywane do obserwacji, monitorowania lub kontrolowania osób, których dane dotyczą, w tym danych gromadzonych za pośrednictwem sieci lub ramach systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie;
    f. dochodzi do dopasowywania lub łączenia zbiorów danych, w szczególności pochodzących z co najmniej dwóch różnych operacji przetwarzania danych, przeprowadzonych w różnych celach lub przez różnych ADO w sposób wykraczający poza uzasadnione oczekiwania osób, których dane dotyczą;
    g. przetwarzanie obejmuje dane osobowe osób wymagających szczególnej opieki, w tym np. dzieci lub pracowników;
    h. następuje innowacyjne wykorzystanie lub stosowanie nowych rozwiązań technologicznych lub organizacyjnych;
    i. samo przetwarzanie uniemożliwia osobom, których dane dotyczą, wykonywanie prawa lub korzystanie z usługi lub umowy.

3. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem ADO przeprowadza pojedynczą ocenę.
4. ADO uwzględnia wykazy rodzajów operacji przetwarzania podlegających lub niepodlegających wymogowi dokonania oceny skutków dla ochrony danych, ustanowione przez organ nadzorczy zgodnie z art. 35 ust. 4 i 5 RODO.
5. W przypadkach, w których nie jest jasne, czy wymagane jest przeprowadzenie oceny skutków dla ochrony danych, ADO przeprowadza taką ocenę.
6. Ocena skutków dla ochrony danych powinna rozpocząć się jak najwcześniej w fazie projektowania operacji przetwarzania. Jeżeli zachodzi taka potrzeba, w szczególności ze względu na zastosowane w projekcie środki techniczne lub organizacyjne, w miarę postępu procesu rozwoju lub w związku z istotną modyfikacją procesu, poszczególne etapy oceny należy powtórzyć.
7. Dokonując oceny skutków dla ochrony danych, ADO konsultuje się z IOD, jeżeli został on powołany, a wyniki konsultacji i podjęte decyzje dokumentuje w ramach oceny skutków dla ochrony danych.
8. Jeżeli dana operacja przetwarzania jest całkowicie lub częściowo realizowana przez Procesora, ADO konsultuje się z Procesorem.
9. Jeżeli uzna to za właściwe, ADO zasięga opinii osób, których dane dotyczą, lub ich przedstawicieli. Jeżeli ostateczna opinia ADO różni się od opinii osób, których dane dotyczą, ADO dokumentuje powody podjęcia bądź niepodjęcia decyzji. ADO uzasadnia także niezasięgnięcie opinii osób, których dane dotyczą, jeśli uzna je za niecelowe.
10. W stosownych przypadkach ADO zasięga opinii niezależnych ekspertów z różnych dziedzin (np. prawników, informatyków, ekspertów z zakresu bezpieczeństwa).
11. W razie potrzeby, przynajmniej gdy zmienia się ryzyko wynikające z operacji przetwarzania, ADO dokonuje przeglądu, by stwierdzić, czy przetwarzanie odbywa się zgodnie z oceną skutków dla ochrony danych.
12. ADO sporządza ocenę skutków dla ochrony danych na piśmie/ w formie elektronicznej.
13. Dokonując oceny skutków dla ochrony danych ADO uwzględnia i dokumentuje co najmniej:
    a. systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie - prawnie uzasadnionych interesów realizowanych przez ADO;
    b. ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
    c. ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą oraz
    d. środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie dotyczących jej przepisów, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy;
    e. ocenę zgodności z kodeksami postępowania.
14. Ocena skutków dla ochrony danych powinna uwzględniać certyfikację, znaki jakości.
15. Jeżeli ocena skutków dla ochrony danych wskaże, że przy braku lub niedostatecznym poziomie planowanych zabezpieczeń środków bezpieczeństwa oraz mechanizmów minimalizujących ryzyko przetwarzanie powodowałoby wysokie ryzyko naruszenia praw lub wolności osób fizycznych, a ADO uznaje, że ryzyka tego nie da się zminimalizować środkami rozsądnymi z punktu widzenia dostępnych

technologii i kosztów wdrożenia, to przed rozpoczęciem przetwarzania ADO konsultuje się z organem nadzorczym.

16. Konsultując się z organem nadzorczym zgodnie z ust. 16, ADO przedstawia mu:
    a. gdy ma to zastosowanie - odpowiednie obowiązki ADO, współadministratorów oraz podmiotów przetwarzających uczestniczących w przetwarzaniu, w szczególności w przypadku przetwarzania w ramach grupy przedsiębiorstw;
    b. cele i sposoby zamierzonego przetwarzania;
    c. środki i zabezpieczenia mające chronić prawa i wolności osób, których dane dotyczą;
    d. dane kontaktowe IOD;
    e. ocenę skutków dla ochrony danych; oraz
17. ADO udziela na żądanie organu nadzorczego wszelkich innych informacji.
18. Projektując operacje przetwarzania, wymagające uprzednich konsultacji, ADO uwzględnia określone w art. 36 ust. 2 RODO terminy na udzielenie przez organ nadzorczy zaleceń lub podjęcie środków naprawczych.
19. ADO uwzględnia zalecenia organu nadzorczego wydane na skutek uprzednich konsultacji i stosuje się do innych środków podjętych przez organ.
20. Ocena jest prowadzono dwuetapowo:

I Etap – badanie w trakcie analizy procesów przetwarzania – zgodnie z Załącznikiem nr 25.

W celu przedstawienia bardziej konkretnego zbioru operacji przetwarzania wymagających przeprowadzenia oceny skutków dla ochrony danych ze względu na ich nieodłączne wysokie ryzyko, uwzględniając poszczególne elementy: art. 35 ust. 1 i art. 35 ust. 3 oraz art.35 ust.4 RODO i motywy 71, 75 i 91 RODO oraz inne wspomniane w RODO odniesienia do operacji przetwarzania, które „mogą powodować wysokie ryzyko", należy wziąć pod uwagę dziewięć następujących kryteriów:

1. Ocena lub punktacja, 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" (motywy 71 i 91 RODO).
2. Automatyczne podejmowanie decyzji o skutku prawnym lub podobnie znaczącym skutku: przetwarzanie mające na celu podjęcie decyzji w sprawie osób, których dane dotyczą, motyw 71 RODO: „w szczególności analizowane lub prognozowane aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się – w celu tworzenia lub wykorzystywania profili osobistych", motyw 75 RODO: „jeżeli przetwarzane są dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych oraz jeżeli przetwarzane są dane genetyczne, dane dotyczące zdrowia lub dane dotyczące seksualności lub wyroków skazujących i naruszeń prawa lub związanych z tym środków bezpieczeństwa". motywy 75, 76, 92, 116 RODO: wywołujących „skutki prawne wobec osoby fizycznej" lub decyzji, które „w podobny sposób istotnie na nią wpływają" (art. 35 ust. 3 lit. a RODO).

3. Systematyczne monitorowanie: przetwarzanie wykorzystywane do obserwacji, monitorowania lub kontrolowania osób, których dane dotyczą, w tym danych gromadzonych za pośrednictwem sieci lub ramach „systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie" (art. 35 ust. 3 lit. c RODO))
4. Dane wrażliwe lub dane o charakterze wysoce osobistym: obejmują szczególne kategorie danych osobowych określone w art. 9 RODO (np. informacje o poglądach politycznych obywateli) oraz dane osobowe dotyczące wyroków skazujących za przestępstwo lub naruszeń prawa zdefiniowane w art. 10 RODO.
5. Dane przetwarzane na dużą skalę, obejmujące:

   - przeprowadzane w ramach określonego systemu;

   - wcześniej zaplanowane, zorganizowane lub mające metodyczny charakter;

   - odbywające się w ramach ogólnego planu gromadzenia danych;

   - realizowane jako część strategii.

6. Dopasowywanie lub łączenie zbiorów danych np. pochodzących z co najmniej dwóch operacji przetwarzania danych przeprowadzonych w różnych celach lub przez różnych administratorów danych w sposób wykraczający poza uzasadnione oczekiwania osób, których dane dotyczą.
7. Dane dotyczące osób wymagających szczególnej opieki, których dane dotyczą: przetwarzanie tego rodzaju danych stanowi jedno z kryteriów ze względu na zwiększoną nierównowagę sił między osobami, których dane dotyczą, a ADO, co oznacza, że osoby fizyczne mogą mieć trudności z wyrażeniem zgody na przetwarzanie swoich danych lub z wyrażeniem sprzeciwu wobec ich przetwarzania, lub mogą mieć trudności z korzystaniem z przysługujących im praw.
8. Innowacyjne wykorzystanie lub stosowanie nowych rozwiązań technologicznych lub organizacyjnych, takich jak połączenie technologii rozpoznającej biometrię.
9. Gdy samo przetwarzanie „uniemożliwia osobom, których dane dotyczą, wykonywanie prawa lub korzystanie z usługi lub umowy" (art. 22 i motyw 91 RODO). Obejmuje to operacje przetwarzania, których celem jest umożliwienie osobom, których dane dotyczą, uzyskania dostępu do usługi lub zawarcia umowy, zmiana tego dostępu lub odmówienie dostępu.

Jeżeli badanie wstępne wykaże, że dany proces może przetwarzać dane z dużym ryzykiem dla praw i wolności podmiotu przetwarzania, proces ten będzie podlegał Etapowi II.

II Etap - Ocena zostanie przeprowadzona zgodnie z wytycznymi Grupy Roboczej art.29 17/PL WP2468 rev.01. – Załącznik nr 28.

1. Ocena zawiera co najmniej:
   a. systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez ADO;
   b. ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
   c. ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, o którym mowa w ust. 1; oraz

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

2. Oceniając – w szczególności do celów oceny skutków dla ochrony danych – skutki operacji przetwarzania wykonywanych przez ADO lub podmiot przetwarzający, uwzględnia się przestrzeganie przez takiego ADO lub taki podmiot przetwarzający zatwierdzonych kodeksów postępowania, o których mowa w art. 40 RODO.
3. W stosownych przypadkach ADO zasięga opinii osób, których dane dotyczą, lub ich przedstawicieli w sprawie zamierzonego przetwarzania, bez uszczerbku dla ochrony interesów handlowych lub publicznych lub bezpieczeństwa operacji przetwarzania.
4. Art. 35 ust 1-7 RODO nie mają zastosowania, jeżeli przetwarzanie na mocy art. 6 ust. 1 lit. c lub e RODO ma podstawę prawną w prawie Unii lub w prawie państwa członkowskiego, któremu podlega administrator, i prawo takie reguluje daną operację przetwarzania lub zestaw operacji, a oceny skutków dla ochrony danych dokonano już w ramach oceny skutków regulacji w związku z przyjęciem tej podstawy prawnej – chyba że państwa członkowskie uznają za niezbędne, by przed podjęciem czynności przetwarzania dokonać oceny skutków dla ochrony danych.
5. W razie potrzeby, przynajmniej gdy zmienia się ryzyko wynikające z operacji przetwarzania, ADO dokonuje przeglądu, by stwierdzić, czy przetwarzanie odbywa się zgodnie z oceną skutków dla ochrony danych.
6. Jeżeli ocena skutków dla ochrony danych, o której mowa w art. 35 RODO, wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby ADO nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania administrator konsultuje się z organem nadzorczym.

§ 17. POLITYKA ZARZĄDZANIA NARUSZENIAMI

1. Naruszenie ochrony danych osobowych oznacza każde naruszenie bez względu na jego przyczynę prowadzące do zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych, a w szczególności:
   a. nieautoryzowany dostęp do danych osobowych;
   b. utratę nośników zawierających dane osobowe;
   c. nieautoryzowaną modyfikację lub zniszczenie danych osobowych;
   d. bezpodstawne udostępnienie danych osobowych;
   e. pozyskiwanie danych osobowych z nielegalnych źródeł.
2. W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub zaistnienia sytuacji, które mogą wskazywać na naruszenie ochrony danych osobowych, każdy członek personelu ADO przerywa wykonywanie czynności związanych z przetwarzaniem danych osobowych i niezwłocznie

informuje o tym fakcie ADO lub bezpośredniego przełożonego, a następnie stosuje się do podjętych przez te osoby decyzji.

3. Powiadomienie o naruszeniu ochrony danych osobowych powinno obejmować:
    a. opis naruszenia ochrony danych osobowych;
    b. określenie sytuacji, miejsca i czasu, w jakim stwierdzono naruszenie ochrony danych osobowych;
    c. określenie wszelkich istotnych informacji mogących wskazywać na przyczynę tego naruszenia;
    d. określenie znanych danej osobie sposobów zabezpieczenia Systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.
4. ADO lub inna upoważniona przez ADO osoba podejmuje wszelkie działania mające na celu:
    a. minimalizację negatywnych skutków zdarzenia i ich późniejsze zupełne usunięcie;
    b. wyjaśnienie okoliczności zdarzenia;
    c. zabezpieczenie dowodów zdarzenia;
    d. umożliwienie dalszego bezpiecznego przetwarzania danych osobowych.
5. W celu realizacji procedury postępowania w przypadku naruszenia ochrony danych osobowych ADO lub wyznaczona przez ADO osoba ma prawo do podejmowania wszelkich działań dopuszczonych przez prawo, a w szczególności:
    a. żądania wyjaśnień od członków personelu;
    b. korzystania z pomocy konsultantów (w tym zewnętrznych podmiotów);
    c. nakazania przerwania pracy, zwłaszcza w zakresie przetwarzania danych osobowych.
6. Odmowa udzielenia przez pracownika wyjaśnień lub współpracy z ADO może być traktowana jako ciężkie naruszenie podstawowych obowiązków pracowniczych w rozumieniu art. 52 § 1 pkt 1) Kodeksu pracy.
7. ADO lub wyznaczona przez ADO osoba, po stwierdzeniu naruszenia ochrony danych osobowych, opracowuje raport końcowy, w którym przedstawia:
    a. okoliczności i charakter powstałego naruszenia, w tym:
        - kategorie i przybliżoną liczbę osób, których danych dotyczy naruszenie,
        - kategorie i przybliżoną liczbę danych osobowych, których dotyczy naruszenie,
        - możliwe konsekwencje powstałego naruszenia,
    b. wnioski i zalecenia ograniczające możliwość wystąpienia podobnego zdarzenia w przyszłości,
    c. opis podjętych działań zaradczych,

    Wzór raportu stanowi Załącznik nr 9 do Polityki Bezpieczeństwa.
8. W przypadku stwierdzenia naruszenia ochrony danych osobowych ADO bez zbędnej zwłoki – nie później jednak niż w terminie 72 godzin od stwierdzenia naruszenia – zgłasza je organowi nadzorczemu. Jeżeli zgłoszenie zostanie dokonane po upływie 72 godzin – należy dołączyć wyjaśnienie przyczyn opóźnienia - wzór zgłoszenia stanowi Załącznik do Polityki Bezpieczeństwa.
9. Jeżeli w zakreślonym wyżej czasie ADO nie jest w stanie zgromadzić i przekazać organowi nadzorczemu wszystkich wymaganych informacji – może ich udzielać sukcesywnie – bez zbędnej zwłoki.
10. Zgłoszenie naruszenia ochrony danych osobowych nie jest wymagane, jeśli jest mało prawdopodobne, aby naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Za dokonanie oceny istnienia lub nieistnienia powyższego ryzyka odpowiada ADO.

11. W sytuacji, kiedy naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych – ADO bez zbędnej zwłoki zawiadamia także osobę, której dane dotyczą, o wystąpieniu naruszenia. Wzór zawiadomienia stanowi Załącznik 9 do Polityki.
12. W zawiadomieniu umieszcza się informacje w zakresie:
    a. imienia i nazwiska oraz danych kontaktowych IOD osobowych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji nt. naruszenia,
    b. konsekwencji naruszenia ochrony danych osobowych, które mogą pojawić się dla osoby, której dane dotyczą w związku z zaistnieniem naruszenia,
    c. środków zastosowanych lub proponowanych przez ADO w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach, także środków w celu zminimalizowania ewentualnych negatywnych skutków naruszenia.
13. Zawiadomienie, o którym mowa w ust. 11, nie jest wymagane w następujących przypadkach:
    a. zostały wdrożone odpowiednie techniczne i organizacyjne środki ochrony, które zostały zastosowane do danych osobowych, których dotyczy naruszenie – w szczególności środki takie jak szyfrowanie uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych;
    b. następnie zostały zastosowane środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
    c. wymagałoby to niewspółmiernie dużego wysiłku – w takim wypadku należy wydać publiczny komunikat lub zastosować podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.
14. Oceny przesłanek wskazanych w ust. 11 dokonuje wyznaczony przez ADO zespół odpowiedzialny za proces zarządzania ryzykiem, według metodyki przyjętej zgodnie z § 8 Polityki. W skład zespołu wchodzą:
    a. przewodniczący,
    b. koordynator zespołu,
    c. właściciele poszczególnych procesów oraz aktywów,
    d. eksperci.

§ 18. ZABEZPIECZENIA, ŚRODKI ORGANIZACYJNE I TECHNICZNE NIEZBĘDNE DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

1. Instrukcja alarmowa.
   Instrukcja definiuje katalog zagrożeń i naruszeń zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Celem instrukcji jest minimalizacja skutków wystąpienia naruszeń bezpieczeństwa, ograniczenie ryzyka powstania zagrożeń i występowania naruszeń w przyszłości.
2. Zagrożenia, naruszenia i sposób reagowania:
    1. Każdy pracownik w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest poinformować bezpośredniego przełożonego lub ADO.
    2. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:
        a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;

b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych;
c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).

3. Do typowych naruszeń bezpieczeństwa danych osobowych należą:
   a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności);
   b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/zagubienie danych);
   c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).
4. W przypadku stwierdzenia wystąpienia zagrożenia, ADO prowadzi postępowanie wyjaśniające w toku, którego:
   a. ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki;
   b. inicjuje ewentualne działania dyscyplinarne;
   c. rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości;
   d. dokumentuje prowadzone postępowania.

   Procedura postępowania na wypadek naruszeń została opisana w Załączniku nr 7.
5. W przypadku stwierdzenia naruszenia, ADO wdraża postępowanie wyjaśniające w toku, którego:
   a. ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały;
   b. zabezpiecza ewentualne dowody;
   c. ustala osoby odpowiedzialne za naruszenie;
   d. podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody),
   e. inicjuje działania dyscyplinarne;
   f. wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości;
   g. dokumentuje prowadzone postępowania.
   h. W/w czynności zostają odnotowane w rejestrze naruszeń ochrony danych będącym Załącznikiem nr 8.

3. Procedura działań korygujących i zapobiegawczych.
   1. Cel procedury
      a. celem procedury jest uporządkowanie i przedstawienie czynności związanych z inicjowaniem oraz realizacją działań korygujących i zapobiegawczych wynikających z zaistnienia incydentów bezpieczeństwa lub zagrożeń systemu ochrony danych osobowych;

b. procedura działań korygujących i zapobiegawczych obejmuje wszystkie te procesy, w których incydenty bezpieczeństwa lub zagrożenia mogą wpłynąć na zgodność z wymaganiami RODO, jak również na poprawne funkcjonowanie systemu ochrony danych osobowych;
c. osobą odpowiedzialną za nadzór nad procedurą jest ADO.

2. Definicje:
   a. Incydent - naruszenie bezpieczeństwa informacji ze względu na poufność, dostępność i integralność.
   b. Zagrożenie – potencjalna możliwość wystąpienia incydentu.
   c. Korekcja – działanie w celu wyeliminowania skutków incydentu.
   d. Działanie korygujące – działanie przeprowadzane w celu wyeliminowania przyczyny incydentu lub innej niepożądanej sytuacji.
   e. Działanie zapobiegawcze – działanie, które należy przedsięwziąć, aby wyeliminować przyczyny zagrożenia lub innej potencjalnej sytuacji niepożądanej.
   f. Kontrola – systematyczna, niezależna i udokumentowana ocena skuteczności systemu ochrony danych osobowych, na podstawie wymagań RODO, Polityki i instrukcji.
3. Opis czynności:
   a. ADO jest odpowiedzialny za analizę naruszeń bezpieczeństwa lub zagrożeń ochrony danych osobowych. Typowymi źródłami informacji o incydentach, zagrożeniach lub słabościach są:
      - zgłoszenia od pracowników,
      - wiedza ADO,
      - wyniki kontroli;
   b. w przypadku, gdy ADO stwierdzi konieczność podjęcia działań korygujących lub zapobiegawczych, ADO/IOD określa: źródło powstania incydentu lub zagrożenia, zakres działań korygujących lub zapobiegawczych, termin realizacji, osobę odpowiedzialną;
   c. ADO/IOD jest odpowiedzialny za nadzór nad poprawnością i terminowością wdrażanych działań korygujących lub zapobiegawczych;
   d. po przeprowadzeniu działań korygujących lub zapobiegawczych, ADO jest zobowiązany do oceny efektywności ich zastosowania;
   e. powyższe czynności ADO/IOD rejestruje zgodnie z Załącznikiem nr 8 oraz sporządza Raport z naruszeń ochrony danych zgodnie z Załącznikiem nr 9.

4. Kontrola systemu ochrony danych osobowych.
   1. Celem procedury jest uporządkowanie i przedstawienie czynności związanych z kontrolą stanu bezpieczeństwa danych osobowych.
   2. Procedura obejmuje wszystkie procesy organizacji, gdzie przestrzeganie zasad ochrony danych osobowych jest wymagane.
   3. Do kontroli stanu ochrony danych osobowych upoważnieni są wyznaczeni przez ADO kontrolerzy wewnętrzni.

4. Kontroli podlegają: systemy informatyczne przetwarzające dane osobowe, zabezpieczenia fizyczne, zabezpieczenia organizacyjne, bezpieczeństwo osobowe oraz zgodność stanu faktycznego z wymaganiami ustawy i aktów wykonawczych.
5. ADO przygotowuje plan kontroli uwzględniając zakres oraz potrzebne zasoby fizyczne, czasowe i osobowe. Kontrola powinna odbyć się co najmniej raz w roku. Kontrolę przeprowadzają powołane przez ADO osoby.
6. Kontrola przeprowadzana jest na podstawie listy kontrolnej dokumentu Załącznik nr 10.
7. Po dokonanej kontroli osoba ją przeprowadzająca przygotowuje i przekazuje raport pokontrolny (Załącznik nr 10.1) kierownikowi kontrolowanej jednostki lub komórki organizacyjnej oraz ADO. Na jego podstawie ADO inicjuje działania korygujące lub zapobiegawcze.

5. Zaznajomienie lub przeszkolenie Użytkowników.
   1. Każdy Użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być zaznajomiony lub przeszkolony w zakresie ochrony danych osobowych zgodnie z nadanym upoważnieniem.
   2. Zaznajomienie polega na udostępnieniu Użytkownikowi w formie elektronicznej lub papierowej materiałów z przepisami prawa dotyczącymi ochrony danych osobowych oraz uregulowaniami obowiązującymi u ADO.
   3. Za zaznajomienie odpowiada ADO, a za jego przeprowadzenie odpowiada wyznaczona przez ADO osoba.
   4. Po zapoznaniu się z materiałami wymienionymi w punkcie 2 lub przeszkoleniu, Użytkownik podpisuje oświadczenie o odbyciu szkolenia/zaznajomieniu się z zasadami ochrony danych osobowych. Oświadczenie zawiera zobowiązanie do przestrzegania zasad ochrony danych.
   5. Dokument ten (Załącznik nr 11) jest przechowywany w aktach osobowych Użytkowników i stanowi podstawę do podejmowania działań w celu nadania im uprawnień do korzystania z systemu informatycznego przetwarzającego dane osobowe.

§ 19. OBOWIĄZEK INFORMACYJNY

Informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą.

1. Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, ADO podczas pozyskiwania danych osobowych podaje jej wszystkie następujące informacje:
    a. swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;
    b. gdy ma to zastosowanie – dane kontaktowe IOD;
    c. cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania;
    d. jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f RODO – prawnie uzasadnione interesy realizowane przez ADO lub przez stronę trzecią;
    e. informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
    f. gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.
2. Poza informacjami, o których mowa w ust. 1, podczas pozyskiwania danych osobowych ADO podaje osobie, której dane dotyczą, następujące inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania:
    a. okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
    b. informacje o prawie do żądania od ADO dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
    c. jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
    d. informacje o prawie wniesienia skargi do organu nadzorczego;
    e. informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
    f. informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.
3. Jeżeli ADO planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym

innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w art. 24 ust. 1, 2 i 3 RODO nie mają zastosowania, gdy – i w zakresie, w jakim – osoba, której dane dotyczą, dysponuje już tymi informacjami.

Informacje podawane w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą.

1. Jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą, ADO podaje osobie, której dane dotyczą, następujące informacje:
   a. swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;
   b. gdy ma to zastosowanie – dane kontaktowe IOD;
   c. cele przetwarzania, do których mają posłużyć dane osobowe, oraz podstawę prawną przetwarzania;
   d. kategorie odnośnych danych osobowych;
   e. informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
   f. gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.
2. Poza informacjami, o których mowa w ust. 1, ADO podaje osobie, której dane dotyczą, następujące informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania wobec osoby, której dane dotyczą:
   a. okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
   b. jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f RODO – prawnie uzasadnione interesy realizowane przez ADO lub przez stronę trzecią;
   c. informacje o prawie do żądania od ADO dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
   d. jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a RODO lub art. 9 ust. 2 lit. a RODO – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
   e. informacje o prawie wniesienia skargi do organu nadzorczego;
   f. źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych;
   g. informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

3. Informacje, o których mowa w ust. 1 i 2, ADO podaje:
   a. w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca – mając na uwadze konkretne okoliczności przetwarzania danych osobowych;
   b. jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą; lub
   c. jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.
4. Jeżeli ADO planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym te dane zostały pozyskane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w ust. 2.
5. Ust. 1– 4 nie mają zastosowania, gdy :
   a. osoba, której dane dotyczą, dysponuje już tymi informacjami;
   b. udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku; w szczególności w przypadku przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem warunków i zabezpieczeń, o których mowa w art. 89 ust. 1 RODO, lub o ile obowiązek, o którym mowa w ust. 1, może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania. W takich przypadkach administrator podejmuje odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osoby, której dane dotyczą, w tym udostępnia informacje publicznie;
   c. pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą; lub
   d. dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy.
6. W celu spełnienia obowiązku informacyjnego ADO prowadzi Rejestr klauzul informacyjnych zgodnie z Załącznikiem nr 16.

§ 20. POSTANOWIENIA KOŃCOWE

1. Polityka Bezpieczeństwa jest dokumentem wewnętrznym i nie może być udostępniania osobom postronnym w żadnej formie.
2. Wszystkie regulacje dotyczące systemów informatycznych określone w Polityce Bezpieczeństwa dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.
3. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce Bezpieczeństwa.
4. Przypadki, nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych.

5. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego
6. w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.
7. Kara dyscyplinarna, orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą o ochronie danych osobowych oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
8. W sprawach nieuregulowanych w niniejszej Polityce Bezpieczeństwa mają zastosowanie przepisy RODO, UODO oraz wydane na jej podstawie akty wykonawcze.
9. Dokumenty powiązanie:

ZAŁĄCZNIK NR 1	WYZNACZENIE INSPEKTORA OCHRONY DANYCH
ZAŁĄCZNIK NR 1.1	ANALIZA WYZNACZENIA IOD
ZAŁĄCZNIK NR 2.1.	OŚWIADCZENIE O ZACHOWANIU POUFNOŚCI
ZAŁĄCZNIK NR 2.2	UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH
ZAŁĄCZNIK NR 3	EWIDENCJA OSÓB UPOWAŻNIONYCH
ZAŁĄCZNIK NR 4	EWIDENCJA OBSZARÓW PRZETWARZANIA
ZAŁĄCZNIK NR 5	WYKAZ ZBIORÓW DANYCH OSOBOWYCH Z OPISEM STRUKTUR
ZAŁĄCZNIK NR 6	EWIDENCJA SYSTEMÓW INFORMATYCZNYCH
ZAŁĄCZNIK NR 7	PROCEDURA POSTĘPOWANIA NA WYPADEK NARUSZEŃ OCHRONY DANYCH OSOBOWYCH
ZAŁĄCZNIK NR 8	REJESTR NARUSZEŃ OCHRONY DANYCH OSOBOWYCH I DZIAŁAŃ KORYGUJĄCYCH I ZAPOBIEGAWCZYCH
ZAŁĄCZNIK NR 9	RAPORT Z NARUSZEŃ OCHRONY DANYCH
ZAŁĄCZNIK NR 10	LISTA KONTROLNA DLA ADO
ZAŁĄCZNIK NR 10.1	RAPORT POKONTROLNY
ZAŁĄCZNIK NR 11	OŚWIADCZENIE O ODBYTYM SZKOLENIU/ZAZNAJOMIENIU Z ZAKRESU OCHRONY DANYCH OSOBOWYCH
ZAŁĄCZNIK NR 12	REJESTR UDOSTĘPNIENIA DANYCH OSOBOWYCH PODMIOTOM ZEWNĘTRZNYM
ZAŁĄCZNIK NR 12.1	WNIOSEK O UDOSTĘPNIENIE DANYCH OSOBOWYCH
ZAŁĄCZNIK NR 13	REJESTR PODMIOTÓW Z KTÓRYMI PODPISANO UMOWY POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH
ZAŁĄCZNIK NR 13.1	LISTA KOKNTROLNA DLA PODMIOTU PRZETWARZAJĄCEGO
ZAŁĄCZNIK NR 13.2	REJESTR KATEGORII CZYNNOŚCI PRZETWARZANIA
ZAŁĄCZNIK NR 14	WZÓR UMOWY POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH
ZAŁĄCZNIK 14.1	WZÓR UMOWY NA UDOSTĘPNIENIE DANYCH OSOBOWYCH
ZAŁĄCZNIK NR 15	TEST RÓWNOWAGI
ZAŁĄCZNIK NR 16	REJESTR KLAUZUL INFORMACYJNYCH

ZAŁĄCZNIK NR 17	REJESTR REALIZACJI ŻĄDAŃ PODMIOTU DANYCH
ZAŁĄCZNIK NR 18	OŚWIADCZENIE PRACOWNIKA, ŻE ZOSTAŁ POINFORMOWANY O WPROWADZENIU MONITORINGU
ZAŁĄCZNIK NR 19	REJESTR UPRAWNIEŃ INFORMATYCZNYCH
ZAŁĄCZNIK NR 19.1	NADANIE UPRAWNIEŃ INFORMATYCZNYCH
ZAŁĄCZNIK NR 20	REJESTR ANONIMIZACJI/UTYLIZACJI/ZNISZCZENIA
ZAŁĄCZNIK NR 20.1.	RAPORT ANONIMIZACJI
ZAŁĄCZNIK NR 21	UMOWA O UDOSTĘPNIENIE WIZERUNKU
ZAŁĄCZNIK NR 22	WYKAZ PROCEDUR
ZAŁĄCZNIK NR 23	POLITYKA RETENCJI
ZAŁĄCZNIK NR 24	INSTRUKCJA ZARZĄDZANIA KOPIAMI ZAPASOWYMI
ZAŁĄCZNIK NR 25	ANALIZA PROCESÓW PRZETWARZANIA
ZAŁĄCZNIK NR 26	LISTA KONTROLNA POZYSKANIA ZGODY NA PRZETWARZANIE DANYCH
ZAŁĄCZNIK NR 27	REJESTR CZYNNOŚCI PRZETWARZANIA
ZAŁĄCZNIK NR 28	OCENA SKUTKÓW DLA OCHRONY DANYCH
ZAŁĄCZNIK NR 29	REGULAMIN ZARZĄDZANIA SKARGAMI I WNIOSKAMI