POLITYKA BEZPIECZEŃSTWA
PRZETWARZANIA DANYCH OSOBOWYCH

ROZDZIAŁ I – POSTANOWIENIA OGÓLNE
ROZDZIAŁ II – DEKLARACJA INTENCJI, CELE I ZAKRES POLITYKI
ROZDZIAŁ III – ZASADY, STANDARDY I WYMAGANIA POLITYKI
ROZDZIAŁ IV – OBOWIĄZKI I ODPOWIEDZIALNOŚĆ W ZAKRESIE ZARZĄDZANIA BEZPIECZEŃSTWEM
ROZDZIAŁ V – OBSZAR PRZETWARZANIA DANYCH I ZBIORY DANYCH OSOBOWYCH
ROZDZIAŁ VI – STRUKTURY ZBIORÓW DANYCH
ROZDZIAŁ VII – ŚRODKI OCHRONY
ROZDZIAŁ VIII – PROCEDURY DOTYCZĄCE PRZETWARZANIA I OCHRONY DANYCH OSOBOWYCH
ROZDZIAŁ IX – POSTANOWIENIA KOŃCOWE

ZAŁĄCZNIKI

Rozdział I – Postanowienia ogólne

§1

Niniejsza „*Polityka bezpieczeństwa przetwarzania danych osobowych*” (dalej jako „**Polityka**”), jest dokumentem, wydanym przez Administratora danych osobowych tj. Fundacja „Gębiczyn” z siedzibą w Gębiczynie (64-707 Gębice), z adresem w Gębiczynie 24, zarejestrowana w rejestrze stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji oraz samodzielnych publicznych zakładów opieki zdrowotnej pod numerem KRS: 0000044887, dla której dokumentację rejestrową prowadzi Sąd Rejonowy Poznań- Nowe Miasto i Wilda w Poznaniu, IX Wydział Gospodarczy KRS, posiadająca numer NIP: 7631662257, REGON: 570316256 (dalej oraz w załącznikach do Polityki zamiennie jako „**Administrator**”; przedmiotowa działalność określana jest natomiast dalej oraz w załącznikach do Polityki zamiennie jako „**Działalność**”) i ma zastosowanie do realizacji zadań w zakresie bezpieczeństwa danych osobowych przetwarzanych przez Administratora w ramach Działalności w celu realizacji założeń rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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) – zwane dalej „**Rozporządzeniem RODO**” – oraz obowiązujących na terenie Rzeczypospolitej Polskiej przepisów prawa krajowego, wydanych w związku z wdrożeniem Rozporządzenia RODO do krajowego porządku prawnego.

Rozdział II – Deklaracja intencji, cele i zakres Polityki

§2

Administrator w ramach Działalności zapewnia bezpieczeństwo przetwarzania danych osobowych (dalej zamiennie jako „**dane**”) oraz wspiera działania i inicjatywy związane z ochroną danych i systemów informatycznych oraz potwierdza cele i zasady bezpieczeństwa informacji w odniesieniu do strategii i wymagań Administratora.

§3

Celem Polityki jest wskazanie działań, jakie Administrator podejmuje się wykonać w celu zabezpieczenia danych osobowych oraz ustanowienie zasad postępowania, które należy stosować, aby zabezpieczyć dane przetwarzane w ramach Działalności przed:

1) przypadkowym lub niezgodnym z prawem zniszczeniem,
2) utratą,
3) modyfikacją,
4) nieuprawnionym ujawnieniem,
5) nieuprawnionym dostępem do danych osobowych,
6) przetwarzaniem z naruszeniem Rozporządzenia RODO.

§4

1. Polityka określa podstawowe zasady bezpieczeństwa i zarządzania bezpieczeństwem danych przetwarzanych tradycyjnie, jak i danych przetwarzanych w systemach informatycznych, przy czym szczegółowe zasady dotyczące przetwarzania danych osobowych przetwarzanych w systemach informatycznych zostały uregulowane w dokumencie pn. *Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych* ustanowionym w ramach Działalności przez Administratora, stanowiącym integralną część dokumentacji dotyczącej ochrony danych osobowych w skali całej Działalności.

2. Polityka dotyczy wszystkich danych osobowych, przetwarzanych w ramach Działalności niezależnie od formy ich przetwarzania oraz tego, czy dane są lub mogą być przetwarzane w zbiorach danych.
3. Wyrażenia lub zwroty niezdefiniowane w Polityce lub jej załącznikach będą mieć znaczenie przypisywane im przez prawo, a przy braku takiej definicji powinny być rozumiane zgodnie ze znaczeniami obowiązującymi w branży teleinformatycznej lub prawniczej (odpowiednio).

Rozdział III – Zasady, standardy i wymagania Polityki

§5

Administrator zapewnia zgodność Polityki z przepisami określającymi zasady przetwarzania danych osobowych, w tym w szczególności z przepisami Rozporządzenia RODO oraz obowiązującymi na terenie Rzeczypospolitej Polskiej przepisami prawa krajowego, w tym także wydanymi w związku z wdrożeniem Rozporządzenia RODO do krajowego porządku prawnego.

§6

Cele Polityki realizowane są poprzez zapewnienie danym osobowym:

1) legalności, rzetelności i przejrzystości – zapewnienie przetwarzania danych zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
2) poufności – zapewnienie, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom;
3) integralności – zapewnienie, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
4) dostępności (przez autoryzowany podmiot) – zapewnienie bycia osiągalnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot;
5) rozliczalności – zapewnienie, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
6) autentyczności – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana (autentyczność dotyczy użytkowników, procesów, systemów i informacji);
7) niezaprzeczalności – zapewnienie braku możliwości wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie;
8) niezawodności – zapewnienie spójności oraz zamierzonych zachowań i skutków;
9) ograniczenia celu – zapewnienie przetwarzania danych w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzania danych dalej w sposób niezgodny z tymi celami;
10) ograniczenia przechowywania – zapewnienie przechowywania danych w formie umożliwiającej identyfikację osoby, której dane dotyczą przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane lub celów archiwalnych, historycznych bądź statystycznych;
11) prawidłowości – zapewnienie, że dane osobowe są prawidłowe i w razie potrzeby usuwanie lub sprostowanie danych nieprawidłowych w świetle celów ich przetwarzania (ustalonych w oparciu o podjęte rozsądne działania mające na celu wykrycie danych nieprawidłowych);
12) minimalizacji – zapewnienie, że zbierane dane są adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, w których są przetwarzane.

§7

Dla skutecznej realizacji Polityki Administrator zapewnia:

1) odpowiednie do zagrożeń i kategorii danych objętych kontrolą, środki techniczne i rozwiązania organizacyjne,
2) opracowanie dokumentacji dotyczącej przetwarzania danych osobowych, w tym w szczególności opracowanie Polityki i Instrukcji,
3) opracowanie i wdrożenie procedur przetwarzania danych osobowych,
4) kształcenie, szkolenie i uświadamianie w dziedzinie bezpieczeństwa, w zakresie przetwarzania danych osobowych i sposobów ich ochrony,
5) okresowe szacowanie zagrożeń dla zbiorów danych osobowych,
6) zarządzanie ciągłością działań biznesowych,
7) regularne monitorowanie, testowanie, ocenianie i uaktualnianie zastosowanych środków ochrony danych osobowych.

Rozdział IV – Obowiązki i odpowiedzialność w zakresie zarządzania bezpieczeństwem

§8

1. Zarządzanie bezpieczeństwem jest procesem ciągłym, realizowanym przy współdziałaniu osób upoważnionych do przetwarzania danych osobowych przez Administratora i – w przypadku jego powołania – z Inspektorem Ochrony Danych (dalej jako „**IOD**").
2. Wszystkie osoby upoważnione do przetwarzania danych zobowiązane są do:
    1) przetwarzania danych osobowych zgodnie z przepisami prawa określającymi zasady ich ochrony, a w szczególności w zgodzie z Rozporządzeniem RODO,
    2) postępowania zgodnie z ustaloną przez Administratora Instrukcją oraz Polityką,
    3) ścisłego przestrzegania zakresu udzielonego upoważnienia do przetwarzania danych osobowych,
    4) zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia,
    5) natychmiastowego zgłaszania Administratorowi (w przypadku powołania IOD zgłoszenie następuje w odniesieniu do IOD we własnej jednostce organizacyjnej), incydentów związanych z naruszeniem bezpieczeństwa danych osobowych oraz przypadków niewłaściwego funkcjonowania systemu,
    6) stosowania ustanowionych przez Administratora procedur dotyczących przetwarzania danych.
3. W przypadku naruszenia przepisów lub zasad postępowania, o których mowa w ust. 2 powyżej, osoba upoważniona do przetwarzania danych osobowych podlega odpowiedzialności służbowej lub karnej.

§9

1. Administrator stwierdza, iż na podstawie art. 37 ust. 1 Rozporządzenia RODO **nie ma obowiązku wyznaczenia IOD**, bowiem:
    a) nie jest on podmiotem publicznym realizującym zadania publiczne,
    b) jego główna działalność nie polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cel wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą i przetwarzanie to nie odbywa się na dużą skalę.
    c) jego główna działalność nie polega na operacjach przetwarzania danych szczególnych kategorii osób (danych wrażliwych), w tym danych dotyczących wyroków skazujących i naruszeń prawa i przetwarzanie to nie odbywa się na dużą

skalę.

2. W przypadku zidentyfikowania w ust. 1 powyżej obowiązku powołania IOD lub pomimo braku obowiązku podjęcia decyzji o powołaniu IOD, Administrator wyznaczy go działając na podstawie art. 37 ust. 4 Rozporządzenia RODO, wskazując jego dane w decyzji o powołaniu IOD, której projekt stanowi załącznik nr 10 do Polityki.
3. Do obowiązków IOD należy w szczególności:
    a) informowanie Administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy Rozporządzenia RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
    b) monitorowanie przestrzegania Rozporządzenia RODO, innych przepisów prawa Unii Europejskiej lub państw członkowskich o ochronie danych oraz Polityki, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
    c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 Rozporządzenia RODO;
    d) współpraca z właściwym organem nadzorczym tj. Prezesem Urzędu Ochrony Danych Osobowych (dalej jako „**Organ Nadzorczy**");
    e) pełnienie funkcji punktu kontaktowego dla Organu Nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 Rozporządzenia RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.
4. **W przypadku nie wyznaczenia IOD – obowiązki, o których mowa w ust. 3 powyżej wykonuje Administrator.**

§10

1. Administrator może powierzyć przetwarzanie danych innemu podmiotowi (dalej jako: „**Outsourcer**"), na podstawie umowy o powierzenie przetwarzania danych.
2. Umowa o powierzenie przetwarzania danych powinna być zawarta na piśmie i określać:
    1) Przedmiot i czas trwania przetwarzania,
    2) Charakter i cel przetwarzania,
    3) Rodzaj danych osobowych powierzonych do przetwarzania,
    4) Kategorie osób, których dane powierzone do przetwarzania dotyczą,
    5) Obowiązki i prawa Administratora,
    6) Zakres obowiązków Outsourcera,
    7) Obowiązek zachowania przez Outsourcera danych w tajemnicy,
    8) Polecenie Administratora do przetwarzania danych,
    9) Podział odpowiedzialności między Administratora, a Outsourcera,
    10) Uprawnienia Administratora w zakresie przeprowadzania audytu i kontroli działalności Outsourcera,
    11) Procedury postępowania z danymi na wypadek zerwania lub wygaśnięcia umowy.
3. Minimalny zakres umowy o powierzenie przetwarzania danych osobowych stanowi załącznik nr 16 do Polityki.
4. Administrator – w sytuacji powierzenia mu przetwarzania danych przez inny podmiot – zgodnie z art. 30 ust. 2 Rozporządzenia RODO prowadzi rejestr kategorii czynności przetwarzania danych osobowych, stanowiący załącznik nr 13 do Polityki, obejmujący co najmniej następujące informacje:
    a. imię i nazwisko lub nazwa oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających;

b. każdego administratora, w imieniu którego działa podmiot przetwarzający, a gdy ma to zastosowanie – przedstawiciela administratora lub podmiotu przetwarzającego oraz inspektora ochrony danych;
c. kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;
d. gdy ma to zastosowanie – przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi Rozporządzenia RODO, dokumentacja odpowiednich zabezpieczeń;
e. o ile jest to możliwe – ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 Rozporządzenia RODO.

Rozdział V – Obszar przetwarzania danych i zbiory danych osobowych

§11

1. Dane osobowe mogą być przetwarzane wyłącznie w pomieszczeniach Administratora, wymienionych w dokumencie pn. „*Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe",* stanowiącym załącznik nr 1 do Polityki.
2. Powyższy wykaz obejmuje zarówno te miejsca, w których wykonuje się operacje na danych osobowych, jak również te, gdzie są przechowywane nośniki informacji zawierające dane.
3. Przetwarzanie danych osobowych przez Administratora następuje przy wykorzystaniu publicznej sieci teleinformatycznej (Internet).
4. W szczególnych wypadkach możliwe jest przetwarzanie danych osobowych poza obszarem wskazanym w ust. 1 powyżej, co wymaga indywidualnej zgody Administratora i musi być usprawiedliwione okolicznościami towarzyszącymi przetwarzaniu danych (np. specyfika stanowiska pracy).
5. Obszary przetwarzania danych osobowych, o których mowa w ust. 1 powyżej są zabezpieczone przed dostępem osób nieupoważnionych do przetwarzania danych poprzez:
   a) ograniczenie możliwości wstępu na teren przedmiotowych obszarów wyłącznie przez osoby posiadające stosowne upoważnienie do przetwarzania danych osobowych;
   b) stosowanie fizycznych zabezpieczeń uniemożliwiających dostęp do obszarów przetwarzania danych osobowych osób nieupoważnionych (drzwi wejściowe do pomieszczeń stanowiących obszar przetwarzania danych osobowych są zamykane na klucz, w którego dyspozycji są wyłącznie osoby posiadające stosowne upoważnienie do przetwarzania danych osobowych; pomieszczenia stanowiące obszar przetwarzania danych osobowych wyposażone są we wzmocnione okna);
   c) nadzór nad osobami nie posiadającymi upoważnienia do przetwarzania danych osobowych przebywającymi w obszarze przetwarzania danych przez osoby posiadające stosowne upoważnienie (zakaz przebywania na obszarze przetwarzania danych osobowych osób nie posiadających upoważnienia do przetwarzania danych osobowych pod nieobecność osoby posiadającej stosowne upoważnienie),
   d) weryfikację tożsamości osób wchodzących na obszary przetwarzania danych osobowych.

§12

1. Dane osobowe mogą być przetwarzane w zbiorach danych, przy zastosowaniu systemów informatycznych (w postaci elektronicznej) oraz zbiorów ewidencyjnych w postaci kartotek, skorowidzów, ksiąg i wykazów (w postaci tradycyjnej – „papierowej").

2. „*Wykaz zbiorów danych osobowych wraz ze wskazaniem formy ich przetwarzania oraz programów używanych do ich przetwarzania*" stanowi załącznik nr 2 do Polityki.

Rozdział VI – Struktury zbiorów danych

§13

1. W ramach prowadzonej Działalności dane osobowe przetwarzane są w zbiorach ewidencyjnych i w systemach informatycznych. *Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi* stanowi załącznik nr 3 do Polityki.
2. Opis wskazuje, jakie kategorie danych są przetwarzane w zbiorach danych.
3. Opis pola danych, którego zawartość może nie być interpretowana jednoznacznie, zawiera obok kategorii, także format zapisu lub określone w danym kontekście znaczenie.
4. Dane osobowe mogą być przesyłane pomiędzy systemami informatycznymi. *Sposób przepływu danych między poszczególnymi systemami informatycznymi*, stanowi załącznik nr 4 Polityki.

Rozdział VII – Środki ochrony

§14

1. Administrator wdraża techniczne i organizacyjne środki, zapewniające odpowiedni stopień bezpieczeństwa odpowiadający ryzyku przetwarzania danych, w tym uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych.
2. Administrator zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia realizacji zasad określonych w § 6 Polityki, w tym: poufności, integralności, dostępności, rozliczalności, autentyczności, niezaprzeczalności oraz niezawodności przetwarzania danych osobowych.
3. *Analiza konieczności przeprowadzenia oceny skutków dla ochrony danych oraz wskazanie zagrożeń, podatności i szacowanego ryzyka dla poszczególnych systemów i zbiorów danych oraz wskazanie zagrożeń, podatności i szacowanego ryzyka dla poszczególnych systemów i zbiorów danych* stanowi załącznik nr 5 Polityki.
4. **IOD przeprowadza raz do roku (do końca grudnia) analizę ryzyka dla poszczególnych systemów informatycznych i zbiorów danych i na tej podstawie przedstawia Administratorowi propozycje w zakresie wyboru organizacyjnych i technicznych środków ochrony, w tym strukturę stosowania zabezpieczeń.** W przypadku braku powołania IOD, czynności, o których mowa w zdaniu poprzedzającym wykonuje Administrator.
5. Analiza ryzyka obejmuje:
    1) identyfikację występujących zagrożeń dla systemów i zbiorów danych osobowych,
    2) określenie wielkości ryzyka tj. prawdopodobieństwa, że określone zagrożenie wykorzysta podatność (słabość) zasobu,
    3) identyfikację obszarów wymagających zabezpieczeń.
4. Zastosowane środki ochrony (organizacyjne i techniczne) powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów i zbiorów danych osobowych.
5. Zawartość załącznika nr 5 do Polityki podlega każdorazowo aktualizacji, po przeprowadzeniu analizy ryzyka.
6. Analiza ryzyka w uzasadnionych przypadkach może być przeprowadzana częściej niż w

trybie określonym w ust. 4 powyżej, za zgodą Administratora, przy czym analizę ryzyka przeprowadza się obligatoryjnie w przypadku:

a) wystąpienia zdarzenia świadczącego o naruszeniu bezpieczeństwa przetwarzania danych osobowych;
b) zmiany w powszechnie obowiązujących przepisach prawa skutkującej koniecznością dostosowania stosowanych środków bezpieczeństwa danych do aktualnych wymogów prawnych;
c) zmian w zakresie Działalności prowadzonej przez Administratora skutkującej zmianą charakteru, zakresu, kontekstu lub celów przetwarzania.

7. IOD, a w przypadku braku jego powołania Administrator:
   a) monitoruje na bieżąco skuteczność zastosowanych środków ochrony danych,
   b) przeprowadza niezbędne zmiany w konfiguracji systemów informatycznych lub procedurach przetwarzania danych w formie tradycyjnej;
   c) przedstawia Administratorowi informacje o stwierdzonych słabościach środków ochrony i wnioski w zakresie ich modyfikacji;
   d) zleca przeprowadzenie niezbędnych zmian w systemach informatycznych lub procedurach przetwarzania danych w formie tradycyjnej.
8. IOD wykonuje czynności, o których mowa w ust. 7 powyżej, samodzielnie lub przy pomocy pracowników oraz współpracowników zatrudnionych przez Administratora. W przypadku braku powołania IOD, czynności, o których mowa w ust. 7 powyżej wykonuje Administrator przy pomocy pracowników oraz współpracowników Administratora.

§15

1. Środki ochrony, zastosowane przez Administratora dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych obejmują:
   1) środki fizyczne,
   2) środki osobowe,
   3) środki techniczne,
2. Środki ochrony fizycznej obejmują:
   1) lokalizacje miejsc przetwarzania danych osobowych w pomieszczeniach o ograniczonym i kontrolowanym dostępie – dostęp do miejsc przetwarzania danych osobowych posiadają wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych, o których mowa w załączniku nr 12 do Polityki przy jednoczesnym zapewnieniu, aby w obszarze przetwarzania danych osobowych osoby nieupoważnione przebywały wyłącznie za zgodą osób upoważnionych oraz w ich obecności,
   2) ustalenie zasad pobierania kluczy do pomieszczeń oraz szaf stanowiących miejsca przetwarzania danych osobowych – Administrator prowadzi ewidencję osób posiadających dostęp do pomieszczeń oraz szaf stanowiących obszar przetwarzania danych osobowych (według wzoru stanowiącego załącznik nr 14 do Polityki),
   3) wyposażenie pomieszczeń, w których przetwarzane są dane osobowe, we wzmocnione drzwi i okna,
   4) składowanie zbiorów danych osobowych (w tym nośników wymiennych i nośników kopii zapasowych) w odpowiednio zabezpieczonych szafach oraz pomieszczeniach.
3. Środki ochrony osobowej obejmują:
   1) dopuszczenie do przetwarzania danych osobowych wyłącznie osób posiadających upoważnienie wydane przez Administratora; *Wzór upoważnienia do przetwarzania danych osobowych*, stanowi załącznik nr 6 Polityki,

2) przeszkolenie osób, o których mowa w pkt. 1) powyżej w zakresie obsługi systemów służących do przetwarzania danych oraz procedur związanych z przetwarzaniem danych w formie tradycyjnej,
3) ustalenie zasad wykonywania pracy i sprawowania nadzoru nad pracą praktykantów, stażystów, wolontariuszy, wykonawców umów, itp.,
4) odebranie od osoby ubiegającej się o dostęp do przetwarzania danych, stosownego oświadczenia o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych, w tym zobowiązania do przestrzegania tych przepisów i zachowania w tajemnicy – także po ustaniu stosunku pracy – wszelkich informacji dotyczących przetwarzania danych osobowych w zbiorach Administratora, a także hasła dostępu do systemu informatycznego – wzór oświadczenia stanowi załącznik nr 11 do Polityki,
5) weryfikację tożsamości osób wchodzących na obszar przetwarzania danych osobowych.

4. Środki ochrony technicznej obejmują:
   1) mechanizmy kontroli dostępu do systemów i zasobów,
   2) zastosowanie odpowiednich i regularnie aktualizowanych narzędzi ochronnych (poziomy dostępu, programy antywirusowe, firewall, itp.),
   3) regularne tworzenie kopii zapasowych zbiorów danych przetwarzanych w systemach informatycznych,
   4) zastosowanie ochrony zasilania w energię elektryczną.
5. Oryginał upoważnienia, o którym mowa w ust. 3 pkt 1) powyżej przekazuje się osobie, na rzecz której zostało ono wystawione. Osoby, o których mowa w zdaniu poprzedzającym zobowiązane są posiadać przedmiotowy dokument w każdym czasie korzystania z dostępu do danych.
6. Oryginały dokumentów, o których mowa w ust. 3 pkt 4) powyżej oraz kopię dokumentów, o których mowa w ust. 3 pkt 1) powyżej, przechowuje IOD, a w przypadku braku jego powołania, Administrator.
7. IOD, a w przypadku braku jego powołania Administrator, w skali całej Działalności prowadzi ewidencję dokumentów, o których mowa w ust. 5 wpisując je do Ewidencji osób upoważnionych do przetwarzania danych przez Administratora stanowiącej załącznik nr 12 do Polityki.
8. Kontrolę poprawności wykonywania czynności, o których mowa w ust. 3 pkt. 1) – 4) w skali całej Działalności – wykonuje IOD, a w przypadku braku jego powołania Administrator.

Rozdział VIII – Procedury dotyczące przetwarzania i ochrony danych osobowych

§ 16

1. IOD, a w przypadku braku jego powołania Administrator, prowadzi rejestr czynności przetwarzania danych osobowych, zwany dalej „**Rejestrem**”.
2. Rejestr prowadzony jest w formie pisemnej i stanowi załącznik nr 7 Polityki.
3. IOD, a w przypadku braku jego powołania Administrator, udostępnia Rejestr na każde żądanie Organu nadzoru.

§ 17

1. Administrator zobowiązany jest do informowania osób, których dane są przez niego przetwarzane, o wszelkich danych wskazanych w art. 13 lub 14 RODO.
2. W celu wykonania zobowiązania wskazanego w ust. 1 powyżej, Administrator wprowadza *Procedurę informowania o przetwarzaniu danych osobowych*, która stanowi załącznik nr 8 do Polityki.

§ 18

1. Administrator ma obowiązek zgłaszania Organowi Nadzoru każdego przypadku naruszenia ochrony danych osobowych.
2. Przez naruszenie ochrony danych osobowych należy rozumieć naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.
3. Administrator zobowiązuje pracowników i współpracowników do niezwłocznego zgłaszania stwierdzenia naruszenia ochrony danych osobowych Administratorowi lub IOD (w przypadku jego powołania).
4. Szczegółowe zasady postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych zawiera *Procedura zgłaszania naruszeń ochrony danych osobowych*, stanowiąca załącznik nr 9 Polityki. Procedura jest przedstawiana każdemu pracownikowi/współpracownikowi Administratora, który na jego polecenie przetwarza dane osobowe.
5. Administrator dokumentuje wszystkie przypadki naruszenia danych osobowych w sposób określony w *Procedurze zgłaszania naruszeń ochrony danych osobowych.*

§ 19

1. Przed podjęciem czynności projektowania jakichkolwiek działań i procesów pracownicy i współpracownicy zobowiązani są do przeprowadzenia konsultacji z IOD, a w przypadku braku jego powołania z Administratorem, co do ochrony danych osobowych w tym:
    a) zakresu danych osobowych, których przetwarzanie będzie konieczne przy realizacji projektu,
    b) istnienia ryzyk naruszenia ochrony danych osobowych,
    c) środków ochrony, jakie winny być stosowane do zabezpieczenia danych w projekcie.
2. Po przeprowadzeniu konsultacji IOD, a w przypadku braku jego powołania Administrator, zgodnie z zasadą *privacy by design*, określa i wdraża środki ochrony (techniczne i organizacyjne) adekwatne do zakresu, kontekstu i celu przetwarzania danych, kosztów wdrożenia, stanu wiedzy technicznej oraz ryzyka naruszenia praw i wolności osób fizycznych.

§ 20

1. Administrator weryfikuje czy dane osobowe podlegają transgranicznym operacjom oraz czy są przekazywane do państw trzecich zgodnie z prawem i zasadą bezpieczeństwa danych. *Weryfikacja transgranicznego przetwarzania danych osobowych oraz przekazywania danych do państw trzecich* stanowi załącznik nr 15 do Polityki.
2. W przypadku przeprowadzania transgranicznych operacji na danych osobowych Administrator wyznaczy wiodący organ nadzorczy.

Rozdział – Postanowienia końcowe

§ 21

1. Administrator opracowuje, aktualizuje i wymienia załączniki do Polityki, w przypadku zmiany informacji w nich zwartych.
2. Ze względu na możliwość nieuprawnionego ujawnienia treści załączników, o których mowa w ust. 1 powyżej, co mogłoby spowodować szkodę dla prawnie chronionych interesów obywateli albo jednostki organizacyjnej, Administrator oznacza je jako informacje niejawne

stanowiące tajemnicę służbową o klauzuli „zastrzeżone” w rozumieniu przepisów ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych (t. j. Dz. U. z 2016 roku poz. 1167 z późn. zm.).

3. Załączniki przechowuje IOD, a w przypadku braku jego powołania Administrator, w pomieszczeniu chroniącym przed dostępem osób nieuprawnionych.

Gębiczyn, dnia _____ r.

Inspektor Ochrony Danych	Administrator

Załączniki

Załącznik nr 1 - Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane obszarów przetwarzania danych

Załącznik nr 2 - Wykaz przetwarzanych zbiorów danych osobowych wraz ze wskazaniem formy ich przetwarzania oraz programów użytych do ich przetwarzania

Załącznik nr 3 - Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

Załącznik nr 4 - Sposób przepływu danych między poszczególnymi systemami informatycznymi,

Załącznik nr 5 - Analiza konieczności przeprowadzenia oceny skutków dla ochrony danych oraz wskazanie zagrożeń, podatności i szacowanego ryzyka dla poszczególnych systemów i zbiorów danych

Załącznik nr 6 - Upoważnienie do przetwarzania danych osobowych,

Załącznik nr 7 - Rejestr czynności przetwarzania danych osobowych,

Załącznik nr 8 - Procedura informowania o przetwarzaniu danych osobowych,

Załącznik nr 9 - Procedura zgłaszania naruszeń ochrony danych osobowych.

Załącznik nr 10 - Wyznaczenie Inspektora Ochrony Danych Osobowych.

Załącznik nr 11 - Oświadczenie o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych.

Załącznik nr 12 - Ewidencji osób upoważnionych do przetwarzania danych osobowych.

Załącznik nr 13 - Rejestr kategorii czynności przetwarzania danych osobowych.

Załącznik nr 14 - Ewidencja osób upoważnionych do dostępu do pomieszczeń i szaf stanowiących miejsca przechowywania danych osobowych.

Załącznik nr 15 - Weryfikacja transgranicznego przetwarzania danych osobowych oraz przekazywania danych do państw trzecich.

Załącznik nr 16 - Minimalny zakres umowy o powierzenie przetwarzania danych osobowych.