Polityka Ochrony Danych Osobowych

Dokument zawiera Politykę Ochrony Danych Osobowych oraz odnośniki do jej załączników.

RODO

Polityka

Spis treści

I. INFORMACJE OGÓLNE

1 Niniejszy dokument stanowi zbiór zasad i regulacji ochrony danych osobowych w PHU MAK-MET STANISŁAW JUŚKIEWICZ.

2 Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO – rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1), zwany dalej Rozporządzeniem Ogólnym/RODO.

3 Polityka Ochrony Danych Osobowych, zwana dalej Polityką Ochrony Danych wprowadzana jest w celu zapewnienia zgodności działań podejmowanych przez Administratora Danych z Ustawą o ochronie danych osobowych oraz Rozporządzeniem Ogólnym.
4 Administratorem danych osobowych jest PHU MAK-MET STANISŁAW JUŚKIEWICZ Z SIEDZIBĄ W OŁAWIE PRZY UL. KASZTANOWEJ 2.

II. DEFINICJE

1 **Administrator/ 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;
2 **Dane osobowe** oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
3 **Dane wrażliwe** oznaczają dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne, dane dotyczące zdrowia, seksualności lub orientacji seksualnej, oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym
4 **Integralność i poufność** oznacza przetwarzanie 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;
5 **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;
6 **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;
7 **Ograniczenie przetwarzania** oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
8 **Podmiot przetwarzający** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora;
9 **Poufność danych** oznacza właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,

10 **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;

11 **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;

12 **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;

13 **Rozporządzenie ogólne, Rozporządzenie** rozumie się rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych

14 **System informatyczny** rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,

15 **Ustawa** – rozumie się przez to ustawę z dnia ….. r. o ochronie danych osobowych [UWAGA: Data ustawy do uzupełnienia jak ustawa zostanie uchwalona]

16 **Usuwanie danych** rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,

17 **Uwierzytelnianie** rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,

18 **Zabezpieczenie danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,

19 **Strona trzecia** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, Administrator, podmiot przetwarzający czy osoby, które - z upoważnienia Administratora lub podmiotu przetwarzającego - mogą przetwarzać dane osobowe;

20 **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;

21 **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;

III. KATALOG INFORMACJI OBJĘTYCH POLITYKĄ BEZPIECZEŃSTWA ORAZ ZAKRES ZASTOSOWANIA

1. Celem wdrożenia niniejszej dokumentacji jest ochrona interesów osób, których dane dotyczą poprzez zapewnienie należytej, adekwatnej do przewidywanych zagrożeń oraz kategorii przetwarzanych danych, ochrony posiadanych zasobów informacyjnych.
2. Wdrożenie niniejszej Polityki Ochrony Danych ma na celu zapewnienie tego by dane osobowe były przetwarzane zgodnie z zasadami RODO, tj.:
    1. w oparciu o podstawę prawną i zgodnie z prawem (legalizm);
    2. rzetelnie i uczciwie (rzetelność);
    3. w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);
    4. w konkretnych celach i nie „na zapas” (minimalizacja);
    5. nie więcej niż potrzeba (adekwatność);
    6. z dbałością o prawidłowość danych (prawidłowość)
    7. nie dłużej niż potrzeba (czasowość);
    8. zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).
3. W celu realizacji ww. zasad, w tym w celu spełnienia wymogów Rozporządzenia ogólnego Administrator Danych Osobowych wdraża odpowiednie środki techniczne i organizacyjne.
4. Administrator uwzględnia ochronę danych i prywatności na każdym etapie tworzenia oraz istnienia technologii obejmujących ich przetwarzanie.
5. Zakres przedmiotowy stosowania niniejszej dokumentacji obejmuje wszystkie zbiory danych osobowych przetwarzane przez Administratora Danych Osobowych, zarówno w formie elektronicznej, jak i papierowej oraz dane osobowe przetwarzane poza zbiorami danych.
6. Zakres podmiotowy stosowania niniejszej dokumentacji obejmuje wszystkich pracowników oraz osoby, przy pomocy których Administrator danych wykonuje swoje czynności, mające dostęp do danych osobowych.
7. Administrator zarządza zmianą mającą wpływ na prywatność w taki sposób, aby umożliwić zapewnienie odpowiedniego bezpieczeństwa danych osobowych oraz minimalizacji ich przetwarzania. W tym celu zasady prowadzenia projektów i inwestycji przez Administratora odwołują się do zasad bezpieczeństwa danych osobowych i minimalizacji, wymagając oceny wpływu na prywatność i ochronę danych, uwzględnienia i zaprojektowana bezpieczeństwa i minimalizacji przetwarzania danych od początku projektu lub inwestycji (privacy by desgin)
8. Dodatkowo, tworzy się Instrukcję postępowania w sprawie realizacji praw osoby, której dane dotyczą. Instrukcja odnosi się do następujących zagadnień:
    1. udzielenia informacji odnośnie przetwarzania danych osobowych,
    2. pozyskiwania danych osobowych (klauzule),
    3. prawa do sprostowania danych osobowych,
    4. prawa do „bycia zapomnianym”,
    5. prawa ograniczenia przetwarzania danych,
    6. prawa do sprzeciwu.
9. Instrukcja postępowania w sprawie w sprawie realizacji praw osoby, której dane dotyczą stanowi załącznik nr 1 do Polityki Ochrony Danych.

10 Dla celów rozliczalności zaleca się dokumentowanie przez Administratora zgłoszeń osób, których dane dotyczą w zakresie zgłaszanych roszczeń, o których mowa w ust. 7.

IV. PODZIAŁ OBOWIĄZKÓW OSÓB ODPOWIEDZIALNYCH ZA OCHRONĘ DANYCH OSOBOWYCH

1 Niniejszy rozdział odnosi się do obowiązków:
    1 Administratora Danych Osobowych,
    2 Inspektora Ochrony Danych Osobowych,
    3 Administratora Systemów Informatycznych,
    4 Innych osób upoważnionych do przetwarzania danych osobowych;

ADMINISTRATOR DANYCH OSOBOWYCH

1 Administratorem Danych Osobowych jest PHU MAK-MET STANISŁAW JUŚKIEWICZ Z SIEDZIBĄ W OŁAWIE PRZY UL. KASZTANOWEJ 2.
2 Do zadań Administratora Danych Osobowych należy:
    1 odpowiedzialność za przestrzeganie zasad związanych z przetwarzaniem danych osobowych, o których mowa w pkt III ust. 2 niniejszej Polityki Ochrony Danych,
    2 powołanie Inspektora Danych Osobowych (fakultatywnie lub obligatoryjnie gdy wystąpiły przesłanki z ust. 8)
    3 powołanie Administratora Systemów Informatycznych (fakultatywnie)
    4 zapewnienie bezpieczeństwa przetwarzanych danych osobowych,
    5 zapewnienie prawidłowego zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych,
    6 nadzór nad przetwarzaniem danych osobowych,
    7 zapewnienie środków technicznych i organizacyjnych niezbędnych dla zapewnienia bezpiecznego przetwarzania danych,
    8 dopuszczanie do przetwarzania danych osobowych wyłącznie osób działających w oparciu o upoważnienie do przetwarzania danych osobowych,
    9 prowadzenie ewidencji osób upoważnionych,
    10 należyte i terminowe udzielanie informacji na wniosek osób, których dane są przetwarzane i które zwróciły się z wnioskiem o udzielenie informacji zgodnie z przepisami Rozporządzenia,
    11 inne obowiązki przewidziane dla Inspektora Danych Osobowych (o ile nie został powołany) i/lub Administratora Systemów Informatycznych (o ile nie został powołany),
    12 inne obowiązki przewidziane w niniejszej Polityce oraz w przepisach prawa krajowego i wspólnotowego.
3 Administrator w sytuacjach przewidzianych niniejszą Polityką i przepisami ochrony danych osobowych, obowiązany jest odpowiadać na wniosek osoby, której dane dotyczą w sytuacji gdy przetwarza jej dane osobowe.
4 W przypadku wykazania przez osobę, której dane osobowe dotyczą, że są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane, Administrator jest obowiązany, bez zbędnej zwłoki, do uzupełnienia, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru.

5 Administrator Danych Osobowych jest obowiązany poinformować bez zbędnej zwłoki innych Administratorów, którym udostępnił zbiór danych, o dokonanym uaktualnieniu lub sprostowaniu danych.

INSPEKTOR OCHRONY DANYCH OSOBOWYCH - PHU MAK-MET NIE POWOŁUJE INSPEKTORA OCHRONY DANYCH OSOBOWYCH

1 Powołanie Inspektora Ochrony Danych Osobowych jest fakultatywne lub obligatoryjne.
2 Obligatoryjne powołanie Inspektora Ochrony Danych Osobowych następuje w sytuacji gdy spełniona została jedna z poniższych przesłanek:
    1 przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;
    2 główna działalność Administratora 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
    3 główna działalność Administratora polega na przetwarzaniu na dużą skalę danych wrażliwych oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa.
3 Fakultatywne powołanie Inspektora Ochrony Danych Osobowych następuje w pozostałych przypadkach niewskazanych w ust. 8. Każdorazowo Administrator powinien ocenić, czy pomimo braku przesłanek z ust. 8, w związku z przetwarzanymi przez siebie danymi, Inspektor powinien być powołany.
4 Wzór powołania Inspektora Ochrony Danych Osobowych znajduje się w załączniku nr 2 pn. „Dokument powołania IODO”
5 Inspektor Ochrony Danych Osobowych 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 ust. 14.
6 Inspektor Ochrony Danych Osobowych może być członkiem personelu Administratora Danych Osobowych lub wykonywać zadania na podstawie umowy o świadczenie usług.
7 Administrator Danych Osobowych publikuje dane kontaktowe Inspektora Ochrony Danych Osobowych i zawiadamia o nich organ nadzorczy.
8 Do zadań Inspektora Ochrony Danych Osobowych należy w szczególności:
    1 informowanie Administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy Rozporządzenia ogólnego oraz innych przepisów Unii lub ustawy o ochronie danych osobowych i doradzanie im w tej sprawie;
    2 monitorowanie przestrzegania przepisów w sprawie ochrony danych osobowych oraz przepisów wewnętrznych dotyczących ochrony danych osobowych obowiązujących u Administratora Danych Osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
    3 udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;
    4 współpraca z organem nadzorczym;
    5 pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z konsultacjami w sprawie oceny skutków dla

ochrony danych oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

9 Inspektor Ochrony Danych Osobowych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.
10 Administrator zapewnia by Inspektor Ochrony Danych Osobowych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.
11 Administrator wspiera Inspektora Ochrony Danych Osobowych w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.
12 Administrator zapewnia by Inspektor Ochrony Danych Osobowych nie otrzymywał instrukcji dotyczących wykonywania tych zadań. Nie jest on odwoływany ani karany przez Administratora ani podmiot przetwarzający za wypełnianie swoich zadań. Inspektor Ochrony Danych Osobowych bezpośrednio podlega najwyższemu kierownictwu Administratora lub podmiotu przetwarzającego.
13 Osoby, których dane dotyczą, mogą kontaktować się z Inspektorem Ochrony Danych Osobowych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy Rozporządzenia.
14 Inspektor Ochrony Danych Osobowych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań.
15 Inspektor Ochrony Danych Osobowych może wykonywać inne zadania i obowiązki. Administrator zapewnia, by takie zadania i obowiązki nie powodowały konfliktu interesów.

ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH

1 Powołanie Administratora Systemów Informatycznych jest fakultatywne.
2 Wzór powołania Administratora Systemów Informatycznych znajduje się w załączniku nr 3 pn. „Dokument powołania ASI”
3 Administrator Systemów Informatycznych odpowiada za zapewnienie przestrzegania zasad ochrony danych osobowych przetwarzanych za pomocą systemów informatycznych określonych w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, w tym w szczególności za:
    1 nadawanie / nadzór nad nadawaniem uprawnień do przetwarzania danych osobowych w systemach informatycznych,
    2 modyfikację w zakresie nadanych uprawnień do przetwarzania danych osobowych w systemach informatycznych,
    3 odbieranie uprawnień do przetwarzania danych osobowych w systemach informatycznych,
    4 nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów,
    5 podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń,
    6 identyfikację i analizę zagrożeń oraz ocenę ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych i tradycyjnych

4 Administrator Systemów Informatycznych podczas wykonywania obowiązków z zakresu ochrony danych osobowych podlega bezpośrednio kierownikowi jednostki organizacyjnej lub Administratorowi.
5 Instrukcja zarządzania systemem informatycznym stanowi załącznik nr 4 do niniejszej Polityki Ochrony Danych.

V. PRZETWARZANIE DANYCH OSOBOWYCH

1 Administrator dokonuje inwentaryzacji danych:
    1 **Dane wrażliwe –** Administrator identyfikuje przypadki, w których przetwarza lub może przetwarzać dane wrażliwe (dane specjalne i dane karne) oraz utrzymuje dedykowane mechanizmy zapewnienia zgodności z prawem przetwarzania danych wrażliwych. W przypadku zidentyfikowania przypadków przetwarzania danych wrażliwych, Administrator postępuje zgodnie z przyjętymi zasadami w tym zakresie,
    2 **Dane niezidentyfikowane -** Administrator identyfikuje przypadki, w których przetwarza lub może przetwarzać dane niezidentyfikowane i utrzymuje mechanizmy ułatwiające realizację praw osób, których dotyczą dane niezidentyfikowane,
    3 **Profilowanie** – Administrator identyfikuje przypadki, w których dokonuje profilowania przetwarzanych danych i utrzymuje mechanizmy zapewniające zgodność tego procesu z prawem. W przypadku zidentyfikowania przypadków profilowania i zautomatyzowanego podejmowania decyzji, Administrator postępuje zgodnie z przyjętymi zasadami w tym zakresie.
    4 **Współadministrowanie –** Administrator identyfikuje przypadki współadministrowania danymi i postępuje w tym zakresie zgodnie z przyjętymi zasadami.
2 Inwentaryzacja danych następuje w ramach Rejestru Czynności Przetwarzania Danych.
3 Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, Administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania, wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa przetwarzania danych osobowych odpowiadający temu ryzyku.

VI. PODSTAWY PRZETWARZANIE DANYCH OSOBOWYCH

1 Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy - i w takim zakresie, w jakim - spełniony jest co najmniej jeden z poniższych warunków:
    1 osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
    2 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;
    3 przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze;

4 przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
5 przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi;
6 przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora 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

2 Przetwarzanie danych osobowych wrażliwych może nastąpić w sytuacji wystąpienia przynajmniej jednej przesłanki.
3 Za prawnie uzasadniony cel Administratora uznaje się w szczególności dochodzenie roszczeń z tytułu prowadzonej działalności oraz marketing bezpośredni własnych produktów lub usług, przy czym przy podejmowaniu działań marketingowych za pomocą środków komunikacji elektroniczne należy stosować przepisy ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną oraz ustawy z dnia 16 lipca 2004 r. prawo telekomunikacyjne, które przewidują dalej idącą ochronę.
4 Zgoda na przetwarzanie danych osobowych, nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.
5 Zgoda na przetwarzanie danych osobowych może obejmować również przetwarzanie danych w przyszłości, jeżeli nie zmienia się cel przetwarzania.
6 Zgoda na przetwarzanie danych osobowych może zostać odwołana w każdym czasie. W przypadku odwołania zgody na przetwarzanie danych osobowych Administrator obowiązany jest usunąć wszystkie dane osobowe osoby, która zgodę cofnęła, chyba że istnieje inna podstawa prawna upoważniająca Administratora do dalszego przetwarzania tych danych dla innych celów niż wskazany w cofniętej zgodzie.
7 Administrator dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.
8 Wskazując ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne/władza publiczna, uzasadniony cel) Administrator dookreśla podstawę w czytelny sposób, gdy jest to potrzebne. Np. dla zgody wskazując na jej zakres, gdy podstawą jest prawo – wskazując na konkretny przepis i inne dokumenty, np. umowę, porozumienie administracyjne, żywotne interesy – wskazując na kategorie zdarzeń, w których się zmaterializują, uzasadniony cel – wskazując na konkretny cel, np. marketing własny, dochodzenie roszczeń.
9 Administrator wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikację na odległość (email, telefon, sms, in.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie itp.).
10 Kierownik komórki organizacyjnej Administratora ma obowiązek znać podstawy prawne, na jakich komórka przez niego kierowana dokonuje konkretnych czynności przetwarzania danych osobowych. Jeżeli podstawą jest uzasadniony interes Administratora, kierownik komórki ma obowiązek znać konkretny realizowany przetwarzaniem interes ADO.

VII. UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator obowiązany jest nadać upoważnienie do przetwarzania danych każdej osobie, która do przetwarzania danych będzie dopuszczona. Upoważnienie może być nadane w formie pisemnej lub elektronicznej.
2. Do nadawania upoważnień w imieniu Administratora umocowany jest STANISŁAW JUŚKIEWICZ.
3. Wzór dokumentu, w oparciu o który Administrator umocowuje osobę inną niż Administrator do nadawania upoważnień stanowi załącznik nr 5 do Polityki Ochrony Danych.
4. Upoważnienie do przetwarzania danych osobowych powinno zawierać:
    1. datę z którą zostało nadane;
    2. datę, z którą upoważnienie wygasa jeżeli jest ono nadane na czas określony;
    3. zakres upoważnienia.
5. Upoważnienie do przetwarzania danych osobowych wygasa z chwilą upływu terminu wypowiedzenia lub rozwiązania umowy zawartej przez Administratora z osobą, której zostało nadane lub w przypadku gdy zostało nadane na czas określony z upływem czasu na jaki zostało nadane.
6. Osoba upoważniona przez Administratora nie ma prawa do nadawania dalszych upoważnień, chyba że upoważnienie do przetwarzania danych osobowych nadane przez Administratora zawiera upoważnienie do nadawania dalszych upoważnień.
7. Wzór upoważnienia do przetwarzania danych stanowi załącznik nr 6 pn. „Upoważnienie do przetwarzania danych i oświadczenie osoby upoważnianej” do niniejszej Polityki Ochrony Danych.
8. Procedura nadawania upoważnień przebiega następująco:
    1. wniosek o wydanie upoważnienia składa OSOBA ZAINTERESOWANA UZYSKANIEM UPOWAŻNIENIA
    2. wniosek może być złożony w formie pisemnej bądź w formie elektronicznej,
    3. przed wydaniem upoważnienia, osoba, której upoważnienie jest wydawane musi zostać zapoznana z zasadami ochrony danych osobowych, w tym z obowiązującymi aktami prawnymi krajowymi i wspólnotowymi, a także z dokumentacją ochrony danych osobowych obowiązującą u Administratora,
    4. za zapoznanie osoby, które upoważnienie jest wydawane odpowiada Administrator
    5. potwierdzenie zapoznania się z zasadami ochrony danych osobowych, osoba upoważniona potwierdza w formie pisemnej lub elektronicznej,
9. Każda osoba, która uzyskała upoważnienie do przetwarzania danych osobowych zobowiązana jest do ich ochrony w sposób zgodny z przepisami Ustawy, Rozporządzenia, Polityki Ochrony Danych oraz Instrukcji zarządzania systemem informatycznym.
10. Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia bądź rozwiązaniu umowy cywilnoprawnej.
11. Wzór oświadczenia osoby upoważnianej w przedmiocie zapoznania, o którym mowa w ust. 8 pkt 5, a także w przedmiocie obowiązków ciążących na ww. osobie w związku z upoważnieniem jej do przetwarzania danych osobowych stanowi załącznik nr 6 pn. „Upoważnienie i oświadczenie”.
12. Ewidencję osób upoważnionych prowadzi DOROTA TRELA - KIEROWNIK BIURA

13 Ewidencja osób upoważnionych może być prowadzona w formie pisemnej bądź elektronicznej
14 Wzór ewidencji osób upoważnionych do przetwarzania danych stanowi Załącznik nr 7 do Polityki Ochrony Danych.
15 Ewidencja zawiera:
    1 imię i nazwisko osoby upoważnionej;
    2 datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych;
    3 identyfikator, jeżeli dane są przetwarzane w systemie informatycznym

Administrator podejmuje działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia Administratora, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie Administratora, chyba że wymaga tego od niej prawo Unii lub prawo państwa członkowskiego.

VIII. REJESTR CZYNNOŚCI PRZETWARZANIA

1 Administrator prowadzi rejestr czynności przetwarzania danych osobowych, za które odpowiada. W rejestrze tym zamieszcza się wszystkie następujące informacje:
    1 imię i nazwisko lub nazwę oraz dane kontaktowe Administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie - przedstawiciela Administratora oraz inspektora ochrony danych;
    2 cele przetwarzania;
    3 opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
    4 kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
    5 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, dokumentacja odpowiednich zabezpieczeń;
    6 jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
    7 jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.
2 Rejestr może mieć formę pisemną, w tym formę elektroniczną.
3 Administrator udostępnia rejestr na żądanie organu nadzorczego.

Wzór rejestru czynności przetwarzania stanowi załącznik nr 8 do Polityki Ochrony Danych.

IX. SZKOLENIA

1 Inspektor Ochrony Danych Osobowych lub inna osoba wyznaczona przez Administratora odpowiada za zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.
2 Zapoznanie jest przeprowadzane przed dopuszczeniem osoby upoważnionej do czynności przetwarzania danych oraz przed nadaniem upoważnienia.
3 W celu zapewnienia stosowania przez pracowników przepisów z zakresu ochrony danych osobowych, Administrator może organizować Szkolenia. Szkolenia prowadzi

Administrator, Inspektor Ochrony Danych Osobowych lub osoba posiadająca wiadomości specjalne z zakresu ochrony danych.

4 Przeprowadzenie szkolenia jest dokumentowane stosownymi zaświadczeniami.

X. OCENA SKUTKÓW PRZETWARZANIA

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

2 Dokonując oceny skutków dla ochrony danych, Administrator konsultuje się z Inspektorem Ochrony Danych Osobowych, jeżeli został on wyznaczony.

3 Ocena skutków dla ochrony danych jest wymagana w szczególności w przypadku:
   1 systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;
   2 przetwarzania na dużą skalę danych osobowych wrażliwych,
   3 systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

4 Ocena zawiera co najmniej:
   1 systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie - prawnie uzasadnionych interesów realizowanych przez Administratora;
   2 ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
   3 ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, oraz
   4 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.

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

Jeżeli ocena skutków dla ochrony danych, wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby Administrator nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania Administrator konsultuje się z organem nadzorczym. Szczegółowa procedura opisana została w art. 36 Rozporządzenia ogólnego.

XI. ZGŁASZANIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1 Szczegółowa procedura opisana została w załączniku do niniejszej Polityki ochrony danych osobowych.

XII. WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

1. Administrator przetwarza dane jedynie na obszarze do tego przeznaczonym w sposób uniemożliwiający dostęp do danych osobom nieuprawnionym.
2. Wykaz budynków, pomieszczeń lub części pomieszczeń wchodzących w skład obszaru, w którym przetwarzane są dane osobowe zawarty został w załączniku nr 9 pn. „Wykaz - obszary".
3. Dodatkowo, wykaz podmiotów, którym dane zostały powierzone, wraz ze wskazaniem obszaru przetwarzania danych znajduje się w Załączniku nr 10 do Polityki Ochrony Danych pn. „Rejestr umów powierzenia".

XIII. PRZEPŁYWY DANYCH OSOBOWYCH

1. Sposób przepływu danych pomiędzy poszczególnymi systemami wskazany został w załączniku nr 11 „Sposób przepływu danych".

XIV. OKREŚLENIE ŚRODKÓW TECHNICZNYCH ORGANIZACYJNYCH NIEZBĘDNNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

1. Każda osoba przetwarzająca dane osobowe zobowiązana jest do zachowania w tajemnicy danych osobowych do których posiada dostęp, sposoby zabezpieczania danych jak również wszelkie informacje, które powzięła w czasie przetwarzania danych, zarówno w sposób celowy, jak i przypadkowy. Obowiązek zachowania danych w tajemnicy jest bezterminowy.
2. Podczas przetwarzania danych trzeba zachować szczególną ostrożność i podjąć wszelkie możliwe środki umożliwiające zabezpieczenie oraz ochronę danych przed nieuprawnionym dostępem, modyfikacją, utratą, zniszczeniem lub ujawnieniem.
3. Hasła i loginy do systemu informatycznego nie mogą być ujawniane nawet po utracie ich ważności.
4. Należy dochować należytej staranności podczas przesyłania dokumentów zawierających dane za pomocą środków komunikacji elektronicznej, w szczególności należy upewnić się czy przesyłane za pomocą poczty elektronicznej dokumenty trafiły do właściwego odbiorcy.
5. W przypadku przesyłania za pomocą środków komunikacji elektronicznej zestawień, spisów czy innych dokumentów zawierających dane osobowe, przesyłany dokument trzeba zaszyfrować, a hasło przesłać, w miarę możliwości innym środkiem komunikacji elektronicznej.
6. Wszelkie dokumenty zawierające dane osobowe powinny być przechowywane w szafach lub pomieszczeniach zamykanych na klucz.
7. Osoba będąca dysponentem kluczy nie może przekazywać kluczy do budynków i pomieszczeń, w których przetwarzane są dane osobom nieuprawnionym, a ponadto obowiązana jest przedsięwziąć działania celem wykluczenia ryzyka ich utraty.
8. Osoba która utraciła posiadane klucze do pomieszczeń Administratora, w których przetwarzane są dane, niezwłocznie zgłasza tą okoliczność Administratorowi lub Inspektorowi Ochrony Danych Osobowych.

9 Inspektor oraz Administrator, w zakresie swoich kompetencji, podejmują wszelkie niezbędne środki techniczne i organizacyjne w celu zabezpieczenia pomieszczenia, do którego klucze utracono.
10 Szczegółowy wykaz środków technicznych, organizacyjnych i bezpieczeństwa stosowanych przez Administratora celem zapewnienia poufności, integralności i rozliczalności a także przetwarzania danych zgodnie z prawem zawarty został w załączniku nr 12 do Polityki Ochrony Danych.
11 W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej należy stosować zasadę tzw. „czystego biurka", co oznacza nie pozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym. Za realizację powyższej zasady odpowiedzialny jest na swym stanowisku każdy z pracowników.
12 Niszczenie dokumentów zawierających dane, brudnopisów, zbędnych kopii odbywa się jedynie za pomocą niszczarki gwarantującej odpowiedni stopień rozdrobnienia lub za pośrednictwem firmy zajmującej się niszczeniem dokumentów, po zawarciu umowy o powierzeniu przetwarzania danych osobowych.
13 Niedopuszczalne jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych.
14 Podczas korzystania z urządzeń wielofunkcyjnych typu ksero, faks, skaner należy zachować szczególną ostrożność. Dokumenty kopiowane bądź skanowane wyjmowane są z urządzenia wielofunkcyjnego niezwłocznie po ich użyciu.
15 Przebywanie osób nieuprawnionych w obszarze, w którym przetwarzane są dane jest dopuszczalne za zgodą Administratora lub w obecności osoby upoważnionej, chyba że dane te są w odpowiedni sposób zabezpieczone przed dostępem.

XV. UMOWA POWIERZENIA

1 Administrator może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych.
2 Podmiot, któremu dane do przetwarzania powierzono, może przetwarzać dane wyłącznie w zakresie i w celu przewidzianym w umowie.
3 Rejestr umów powierzenia prowadzi DOROTA TRELA - KIEROWNIK BIURA
4 Wzór Rejestru umów powierzenia stanowi załącznik nr 10 do Polityki Ochrony Danych.
5 Umowa powierzenia powinna być zawarta w formie pisemnej, w tym w formie elektronicznej.
6 Umowa powierzenia powinna zawierać następujące informacje, zgodnie z którymi podmiot przetwarzający:
    1 przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora - 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 Administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;

2. zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
3. podejmuje wszelkie środki wymagane Rozporządzeniem ogólnym,
4. przestrzega warunków korzystania z usług innego podmiotu przetwarzającego,
5. biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga Administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw;
6. uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga Administratorowi wywiązać się z obowiązków określonych w Ogólnym Rozporządzeniu;
7. po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji Administratora 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;
8. udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym ustępie oraz umożliwia Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich;
9. podmiot przetwarzający niezwłocznie informuje Administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie Ogólnego rozporządzenia lub innych przepisów Unii lub państwa członkowskiego o ochronie danych.

7. Wzór umowy powierzenia stanowi załącznik nr 13 do niniejszej Polityki Ochrony Danych.

XVI. KONTROLA PRZESTRZEGANIA ZASAD DOTYCZĄCYCH PRZETWARZANIA DANYCH OSOBOWYCH

1. Kontrolę nad ochroną przetwarzanych danych osobowych sprawuje Administrator.
2. W przypadku gdy powołano Inspektora Ochrony Danych Osobowych lub Administratora Systemów Informatycznych, nadzór i kontrolę nad ochroną danych osobowych przetwarzanych w [nazwa podmiotu] sprawuje Inspektor Ochrony Danych Osobowych oraz Administrator Systemów Informatycznych - w odniesieniu do danych osobowych przetwarzanych w systemach informatycznych służących do przetwarzania danych osobowych.
3. Inspektor Ochrony Danych Osobowych czynności kontrolne dokonuje w ramach sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych i wewnętrznymi przepisami dotyczącymi ochrony danych osobowych obowiązującymi u Administratora.
4. Inspektor Ochrony Danych Osobowych może przeprowadzić na polecenie Administratora sprawdzenie w trybie:
    1. sprawdzenia planowego - według opracowanego planu sprawdzeń;
    2. sprawdzenia doraźnego - w przypadku nieprzewidzianym w planie sprawdzeń, w sytuacji powzięcia wiadomości o naruszeniu ochrony danych osobowych lub uzasadnionego podejrzenia wystąpienia takiego naruszenia, niezwłocznie po powzięciu takich informacji;

5 Inspektor Ochrony Danych Osobowych opracowuje plan sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych.
6 Po zakończeniu sprawdzenia, Inspektor Ochrony Danych Osobowych przygotowuje dla Administratora, sprawozdanie w tym zakresie. Sprawozdanie sporządzane jest w postaci elektronicznej albo w postaci papierowej.
7 Inspektor Ochrony Danych Osobowych ma prawo do kontroli podmiotów, którym powierzono przetwarzanie danych osobowych w trybie określonym w Polityce Bezpieczeństwa, o ile w umowie o powierzeniu przetwarzania danych osobowych istnieją stosowne zapisy w tym zakresie.
8 Wzór sprawozdania ze sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych stanowi Załącznik nr 14 do Polityki Ochrony Danych.

Jeśli Inspektor Ochrony Danych Osobowych nie został powołany, Administrator nie ma obowiązku tworzenia planu sprawdzeń ani przygotowywania sprawozdania ze sprawdzenia.

XVII. POSTANOWIENIA KOŃCOWE

1 Dokumentacja przetwarzania danych osobowych stanowi wewnętrzną regulację Administratora i obowiązuje wszystkich pracowników i współpracowników Administratora oraz inne osoby przetwarzające dane osobowe przetwarzane przez Administratora.
2 Dokumentacja przetwarzania danych osobowych obowiązuje od dnia jej wprowadzenia w życie w sposób przyjęty u Administratora. Wszelkie zmiany obowiązują od dnia ich wprowadzenia w życie w sposób przyjęty u Administratora.
3 Nieuzasadnione zaniechanie obowiązków wynikających z niniejszego dokumentu może stanowić podstawę do uznania, że doszło do ciężkiego naruszenia obowiązków pracowniczych lub niewykonania zobowiązania w przypadku stosunku prawnego innego niż stosunek pracy.
4 W sprawach nieuregulowanych mają zastosowanie przepisy powszechnie obowiązującego prawa, w tym w szczególności przepisy ustawy i Rozporządzenia Ogólnego.

XVIII. ZAŁĄCZNIKI

Załącznik nr 1 - Instrukcja postępowania w sprawie ochrony danych osobowych:

- Procedura dot. Prawa do Bycia Zapomnianym
- Procedura dot. Prawa do Informacji i Prawo Dostępu do Danych
- Procedura dot. Prawa do Ograniczenia Przetwarzania Danych
- Procedura dot. Prawa do Przenoszenia Danych
- Procedura dot. Prawa do Sprostowania Danych
- Procedura dot. Prawa Sprzeciwu

Załącznik nr 2 - Dokument Powołania Inspektora Ochrony Danych Osobowych
Załącznik nr 3 - Dokument Powołania Administratora Systemów Informatycznych
Załącznik nr 4 – Procedura Zarządzania Systemem Informatycznym
Załącznik nr 5 - Dokument Umocowania w Przedmiocie Wydania Upoważnień
Załącznik nr 6a - Upoważnienie do przetwarzania danych osobowych
Załącznik nr 6b – Oświadczenie zapoznania się z przepisami dotyczącymi danych osobowych
Załącznik nr 7 - Ewidencja osób upoważnionych do przetwarzania danych osobowych
Załącznik nr 8 - Rejestr czynności przetwarzania

Załącznik nr 9 - Wykaz obszarów przetwarzania
Załącznik nr 10 - Rejestr umów powierzenia
Załącznik nr 11 - Sposób Przepływu Danych Osobowych
Załącznik nr 12 - Środki organizacyjne, techniczne, bezpieczeństwa
Załącznik nr 13 - Umowa Powierzenia
Załącznik nr 14 - Sprawozdanie z Kontroli Zgodności
Załącznik nr 15 – Rejestr Naruszeń
Załącznik nr 16 – Polityka Kluczy
Załącznik nr 16a – Ewidencja osób upoważnionych do dysponowania kluczami
Załącznik nr 17 – Procedura zgłaszania naruszeń ochrony danych osobowych
Załącznik nr 18 – Techniczny audyt – wykaz nośników elektronicznych

---