Nazwa jednostki	ZESPÓŁ SZKÓŁ W DZWOLI
Dokument	**POLITYKA OCHRONY DANYCH OSOBOWYCH W ZESPOLE SZKÓŁ W DZWOLI**

POLITYKA OCHRONY DANYCH OSOBOWYCH W ZESPOLE SZKÓŁ W DZWOLI, DZWOLA 121 B, 23-304 DZWOLA

Podpis Administratora

…….

SPIS TREŚCI

A. POSTANOWIENIA OGÓLNE

1. PODSTAWOWE DEFINICJE

Użyte w Polityce pojęcia oznaczają:

1) Administrator/ Administrator Danych – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Administratorem danych osobowych przetwarzanych jest ZESPÓŁ SZKÓŁ W KOCUDZY;

2) Administrator Systemów Informatycznych (ASI) – osoba wyznaczona przez Administratora Danych, koordynująca działania związane z zapewnieniem bezpieczeństwa systemów informatycznych, w tym również odpowiadająca za nadzór nad zabezpieczeniem danych osobowych przetwarzanych w systemach informatycznych wykorzystywanych przez Administratora Danych;

3) Analiza ryzyka – proces dążący do określenia charakteru i poziomu ryzyka;

4) Dane osobowe – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"), gdzie poprzez możliwą do zidentyfikowania osobę fizyczną rozumie się osobę, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

5) DPIA – ocena skutków dla ochrony danych osobowych (*data protection impact assessment*);

6) Hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie;

7) Inspektor Ochrony Danych (IOD) – osoba wyznaczona przez Administratora Danych, koordynująca procesy związane z przestrzeganiem zasad ochrony danych osobowych w ramach procesów przetwarzania danych osobowych zachodzących w strukturze Administratora Danych;

8) Odbiorca – osoba fizyczna lub prawna, organ publiczny, jednostka 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

Europejskiej 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 co celów przetwarzania;

9) Osoba upoważniona – osoba posiadająca formalne upoważnienie wydane przez Administratora Danych lub osoba przez niego wyznaczona;

10) Organ nadzorczy – niezależny organ publiczny w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych osobowych w Unii, powołany w każdym państwie członkowskim Unii, którego podstawowym zadaniem jest monitorowanie stosowania RODO;

11) Państwo trzecie – państwo nienależące do Europejskiego Obszaru Gospodarczego;

12) Podmiot przetwarzający –osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora;

13) Pracownik – osoba współpracująca z Administratorem Danych na podstawie umowy o pracę lub umowy cywilnoprawnej;

14) Przetwarzanie – operacja 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;

15) Pseudonimizacja – 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;

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

17) 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;

18) Unia – Unia Europejska;

19) UODO – Urząd Ochrony Danych Osobowych;

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

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.

2. CEL POLITYKI OCHRONY DANYCH OSOBOWYCH

1. Niniejsza Polityka ochrony danych osobowych wraz z załącznikami stanowi obowiązującą dokumentację w zakresie wdrażania, przestrzegania i weryfikacji zasad ochrony danych osobowych.
2. Polityka została opracowana i wdrożona w strukturze Administratora Danych w celu zapewnienia zgodności przetwarzania danych osobowych z wymogami obowiązujących w tym zakresie polskich i europejskich aktów prawnych, w szczególności:
    1) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),
    2) Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2018 r., poz. 1000 ze zm.).
    3) Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247)
    4) Przepisów szczególnych, regulujących funkcjonowanie Jednostki i przetwarzanych w ramach jej działalności danych osobowych.
    5) Dobrych praktyk z zakresu bezpieczeństwa informacji oraz ochrony danych osobowych.
3. Celem Polityki Ochrony Danych jest zapewnienie ochrony danych osobowych przed wszelakiego rodzaju zagrożeniami, tak wewnętrznymi, jak i zewnętrznymi, świadomymi lub nieświadomymi. Określa zasady postępowania w związku z przetwarzaniem danych osobowych. Odnosi się zarówno do przetwarzania danych osobowych w formie papierowej (tradycyjnej), jak i w systemach informatycznych.
4. 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:
    1) Poufność danych - oznacza, że jest ona dostępna wyłącznie dla osób, które zostały upoważnione do korzystania z danej informacji;
    2) Dostępność danych - oznacza możliwość wykorzystania zasobu przez upoważnioną osobę, na każde uzasadnione żądanie, w ustalonym czasie;

3) Integralność danych - oznacza, że informacja nie uległa zmianie od czasu ostatniej autoryzowanej modyfikacji lub nie została usunięta w niekontrolowany sposób;

4) Autentyczność - właściwość polegającą na tym, że pochodzenie lub zawartość danych jest taka jak deklarowana;

5) Niezaprzeczalność - brak możliwości zanegowania swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie;

6) Rozliczalność - właściwość pozwalająca przypisać określone działanie do osoby fizycznej lub procesu oraz umiejscowić je w czasie.

5. Dokumentacja regulująca prawidłowość, zgodność z prawem przetwarzania danych osobowych obowiązuje wszystkich pracowników Administratora Danych, którzy w zakresie swoich obowiązków służbowych przetwarzają dane osobowe, jak również innych osób, które z upoważnienia Administratora Danych uzyskały dostęp do danych osobowych.
6. Każda z tych osób została zapoznana z najważniejszymi procedurami bezpieczeństwa danych opisanymi w Polityce ochrony danych osobowych i zobowiązana do ich przestrzegania w zakresie wynikającym z przydzielonych zadań. Osoby, o których mowa złożyły oświadczenie o zapoznaniu się z procedurami bezpieczeństwa danych oraz zobowiązały się do ich stosowania.
7. Wszelkie wątpliwości dotyczące sposobu interpretacji zapisów Polityki ochrony danych osobowych, powinny być rozstrzygane na korzyść zapewnienia możliwie najwyższego poziomu ochrony danych osobowych oraz realizacji praw osób, których dane dotyczą. W przedmiocie spraw nieuregulowanych Polityką Ochrony Danych, zastosowanie znajdują przepisy prawa powszechnie obowiązującego.
8. Polityka Ochrony Danych wraz z załącznikami wchodzi w życie z dniem jej podpisania przez osoby uprawnione do reprezentacji Administratora Danych.

3. ZAKRES STOSOWANIA POLITYKI

1. Polityka ochrony danych określa sposób przetwarzania danych osobowych i zarządzania procesami związanymi z przetwarzaniem danych osobowych w celu zapewnienia odpowiedniej ochrony tych danych. Jest to zestaw praw, reguł i praktycznych doświadczeń dotyczących sposobu zarządzania, ochrony i dystrybucji danych osobowych wewnątrz Administratora Danych.

2. Polityka odnosi się całościowo do problemu zabezpieczenia danych osobowych, tj. zarówno do zabezpieczenia danych przetwarzanych tradycyjnie, jak i danych przetwarzanych w systemach informatycznych.

3. Politykę ochrony danych osobowych stosuje się do wszelkich czynności, stanowiących w myśl RODO, przetwarzanie danych osobowych. Polityka ma zastosowanie do przetwarzania danych osobowych, niezależnie od:

1) sposobu przetwarzania (całkowicie zautomatyzowany, częściowo zautomatyzowany lub inny niż zautomatyzowany),
2) formy lub postaci przetwarzania (papierowa, elektroniczna lub inna),
3) kanałów przepływu danych osobowych,
4) narzędzi informatycznych służących do przetwarzania danych osobowych (systemów, aplikacji, programów),
5) celu przetwarzania,
6) źródła pochodzenia danych osobowych,
7) kategorii danych osobowych.

4. Polityka określa obowiązki i odpowiedzialność osób zobowiązanych do realizacji zadań związanych z procesami.

5. Politykę stosują wszystkie osoby, które na polecenie Administratora uczestniczą w przetwarzaniu danych osobowych.

4. DEKLARACJA ADMINISTRATORA

1. Administrator Danych – ZESPÓŁ SZKÓŁ W DZWOLI, świadomy wagi zagrożeń jakie niesie za sobą przetwarzanie danych osobowych dla wolności i praw osób, których dane dotyczą, uznaje ochronę tych danych, w szczególności zapewnienie ich bezpieczeństwa, za jeden z priorytetów działalności.
2. Administrator Danych podejmuje działania mające na celu wdrożenie przepisów o ochronie danych osobowych oraz zapewnienie stałej zgodności działalności z tymi przepisami.
3. Administrator Danych:
   1) wdraża, utrzymuje i udoskonala ochronę danych osobowych, której celem jest zapewnienie realizacji praw i wolności osób, których te dane dotyczą;
   2) systemowo identyfikuje ryzyka dla bezpieczeństwa danych osobowych oraz minimalizuje ryzyka, przez zastosowanie adekwatnych środków organizacyjnych i technicznych;
   3) wspiera IOD w wypełnianiu przez niego zadań, zapewniając mu w niezbędnym zakresie zasoby do ich wykonania, dostęp do informacji mających wpływ na ochronę danych osobowych i dostęp do operacji przetwarzania, w szczególności przez niezwłoczne włączanie IOD we wszystkie sprawy dotyczące ochrony danych osobowych, a także przez zapewnienie zasobów niezbędnych do utrzymania jego wiedzy fachowej;
   4) reaguje na naruszenia ochrony danych osobowych oraz wdraża środki zapobiegające ich wystąpieniu w przyszłości.
4. Administrator Danych zapewnia:
   1) merytoryczną podległość IOD bezpośrednio Administratorowi Danych,
   2) niezależność IOD w zakresie wykonywanych obowiązków, co oznacza, że nie może on otrzymywać instrukcji dotyczących wykonywania swoich zadań oraz nie może zostać ukarany za wypełnianie swoich zadań, ani z tego powodu odwołany,
   3) powierzanie IOD tylko takich zadań i obowiązków, które nie pozostają w konflikcie interesów.
5. Administrator Danych oczekuje, że zasady i procedury określone w niniejszym dokumencie będą faktycznie wdrożone i stosowane przez ich adresatów.
6. Zobowiązuje się wszystkie osoby dopuszczone do przetwarzania danych osobowych do dostosowania ich postępowania do wymogów wynikających z niniejszej Polityki ochrony danych osobowych.

5. OBSZAR PRZETWARZANIA DANYCH OSOBOWYCH

1. Obszar przetwarzania danych osobowych obejmuje budynki i znajdujące się w nich pomieszczenia, w których przetwarzane są dane osobowe, w tym:

1) miejsca, w których wykonywane są operacje na danych osobowych, realizowane w postaci papierowej lub elektronicznej, w tym w systemach teleinformatycznych;
2) miejsca, w których przechowuje się wszelkie nośniki informacji zawierające dane osobowe, w tym dokumentację papierową, nośniki komputerowe, urządzenia służące do przetwarzania danych osobowych, w tym komputery, serwery, macierze dyskowe;
3) pomieszczenia, gdzie składowane są uszkodzone komputerowe nośniki danych, zawierające dane osobowe.

2. Wykaz obszarów przetwarzania wraz z opisem środków technicznych stosowanych do zabezpieczenia danych osobowych stanowi zał. nr 1 do niniejszej Polityki.

6. ZAKRES PRZETWARZANYCH DANYCH OSOBOWYCH

1. Polityka ma zastosowanie w stosunku do wszystkich danych osobowych przetwarzanych przez Administratora Danych, niezależnie od formy ich przetwarzania (elektroniczna lub papierowa) oraz tego, czy są to dane przetwarzane w zbiorach danych, w zestawach czy stanowią one pojedyncze informacje osobowe.

2. W celu przestrzegania zasady rozliczalności Administrator Danych prowadzi:

1) rejestr czynności przetwarzania danych osobowych, których jest Administratorem,
2) rejestr kategorii czynności przetwarzania dokonywanych w imieniu Administratorów, którzy powierzyli mu przetwarzanie danych.

3. Rejestr czynności przetwarzania danych osobowych, zawiera co najmniej następujące informacje:

1) nazwę oraz dane kontaktowe Administratora Danych oraz wszelkich współadministratorów;
2) gdy ma to zastosowanie imię, nazwisko lub nazwę oraz dane kontaktowe swojego przedstawiciela (jeśli wyznaczono);
3) imię i nazwisko oraz dane kontaktowe IOD;
4) nazwy czynności przetwarzania;
5) cele przetwarzania;
6) opis kategorii osób, których dane dotyczą;
7) opis kategorii danych osobowych;
8) planowany termin usunięcia kategorii danych;

9) nazwę współadministratora i dane kontaktowe (jeśli dotyczy);
10) nazwę podmiotu przetwarzającego i dane kontaktowe (jeśli dotyczy);
11) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
12) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń;
13) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

4. Rejestr kategorii czynności przetwarzania, zawiera co najmniej następujące informacje:

1) nazwę i dane kontaktowe podmiotu, który powierzył przetwarzanie;
2) powód/ Uzasadnienie i podstawy prawne, nazwa umowy/porozumienia;
3) datę obowiązywania powierzenia;
4) rodzaj i kategorie przetwarzanych danych;
5) zakres przetwarzanych danych;
6) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

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

6. Wzór rejestru czynności przetwarzania stanowi załącznik nr 2 do Polityki.

7. Wzór rejestru kategorii czynności przetwarzania stanowi załącznik nr 3 do Polityki.

8. Rejestr czynności przetwarzania oraz rejestr kategorii czynności przetwarzania przyjmują formę pisemną w tym formę elektroniczną, która powinna być prowadzona w systemie informatycznym równolegle z formą pisemną.
9. Administrator jest zobowiązany do udostępnienia w/w rejestrów na żądanie organu nadzorczego. W/w rejestry nie stanowią dokumentów udostępnianych na podstawie Ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej.
10. IOD we współpracy z Administratorem przygotowuje i aktualizuje rejestry o których mowa powyżej.

7. ORGANIZACYJNE ŚRODKI OCHRONY DANYCH OSOBOWYCH

1. W celu zapewnienia zgodności przetwarzania danych osobowych z przepisami RODO Administrator Danych wdraża środki organizacyjne obejmujące w szczególności:

1) organizację systemu ochrony danych osobowych, z określeniem ról, zadań i odpowiedzialności;
2) Politykę ochrony danych, a także powiązane z nią procedury i instrukcje;
3) okresowe przeglądy Polityki oraz dokumentów powiązanych, nie rzadziej niż raz na rok;
4) procedury wydawania upoważnień do przetwarzania danych osobowych;
5) zarządzanie naruszeniami ochrony danych osobowych, zgodnie z procedurą;
6) procedury zarządzania uprawnieniami w systemach teleinformatycznych służących do przetwarzania danych osobowych;
7) podnoszenie świadomości pracowników w zakresie ochrony danych osobowych;
8) procedury zapewniające realizację obowiązków informacyjnych;
9) procedury zapewniające realizację praw osób, których dane dotyczą;

2. W razie konieczności, w oparciu o wyniki analizy ryzyka, stosuje się dodatkowo inne organizacyjne środki ochrony danych osobowych.

8. TECHNICZNE ŚRODKI OCHRONY DANYCH OSOBOWYCH

1. W celu zabezpieczenia danych osobowych przed udostępnieniem osobom nieupoważnionym, zabraniem przez osoby nieuprawnione, przetwarzaniem z naruszeniem prawa oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, Administrator Danych wdraża techniczne środki ochrony danych osobowych odpowiednie do zagrożeń oraz kategorii danych osobowych oraz niezbędne zabezpieczenia.

2. Szczegółowe wymagania w zakresie stosowania wskazanych środków ochrony oraz niezbędnych zabezpieczeń określone są w politykach szczegółowych, instrukcjach i procedurach dotyczących:

1) bezpieczeństwa teleinformatycznego;
2) ciągłości działania;
3) bezpieczeństwa fizycznego.

9. OGÓLNE ZASADY BEZPIECZEŃSTWA OCHRONY DANYCH

1. Dostęp do danych osobowych mogą mieć tylko pracownicy posiadający upoważnienie do ich przetwarzania.
2. Przebywanie osób nieuprawnionych do przetwarzania danych w pomieszczeniu, w którym przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do ich przetwarzania, chyba, że dane te są w odpowiedni sposób zabezpieczone przed dostępem.
3. Pracownicy mający dostęp do danych osobowych nie mogą ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem, w zakresie obowiązków służbowych, w ramach udzielonego upoważnienia do przetwarzania danych.
4. Pracownicy przechowujący dane osobowe zobowiązani są do zabezpieczenia materiałów zawierających dane w sposób uniemożliwiający dostęp do nich osobom nieuprawnionym.
5. Niedopuszczalnym jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia oraz jej bezpośredni przełożony.
6. Nikomu nie należy udostępniać indywidualnych haseł i identyfikatorów do systemów informatycznych.
7. Wysyłanie seryjnych wiadomości e-mail wymaga zastosowania opcji kopia ukryta.
8. Nie można udzielać informacji dotyczących danych osobowych innym podmiotom na podstawie prośby o takie dane skierowanej w formie zapytania telefonicznego.
9. W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej pracownicy zobowiązani są do stosowania zasady tzw. czystego biurka, która oznacza niepozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym. Za realizację powyższej zasady odpowiedzialny jest na swym stanowisku każdy z pracowników. Nie należy pozostawiać danych osobowych w miejscach ogólnodostępnych takich jak np. biurka, blaty, parapety.
10. Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe odbywać się musi w sposób uniemożliwiający odczytanie zawartej w nich treści, np. z wykorzystaniem niszczarek.

11. Za bezpieczeństwo przetwarzania danych osobowych w określonym zbiorze indywidualną odpowiedzialność ponosi przede wszystkim każdy pracownik mający dostęp do danych.
12. W czasie chwilowej nieobecności pracowników w pomieszczeniach, w godzinach pracy jak i po zakończeniu pracy, są oni zobowiązani do zamykania na klucz pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe.
13. Klucze do pomieszczeń, w których przetwarzane są dane osobowe nie mogą być pozostawione w zamku w drzwiach. Pracownicy zobowiązani są do dołożenia należytej staranności w celu zabezpieczenia kluczy przed udostępnieniem ich osobom nieupoważnionym.
14. Przed wyjściem z pomieszczenia, w którym przechowywane są dane osobowe należy upewnić się, że zostało ono odpowiednio zabezpieczone (zamknięte okna, drzwi).
15. Po zakończeniu pracy w systemie informatycznym, w którym przechowywane są dane osobowe, należy wylogować się z systemu.
16. Osoba użytkująca komputer przenośny zawierający dane osobowe zobowiązana jest do zachowania szczególnej ostrożności podczas jego transportu, przechowywania i użytkowania poza obszarem, w którym przetwarzane są dane osobowe.
17. Na pracowniku pracującym zdalnie spoczywa obowiązek odpowiedniego zabezpieczenia danych tak, aby osoby trzecie nie miały dostępu do danych osobowych.
18. Dane osobowe przesyłane elektronicznie powinny być zabezpieczone hasłem. Hasło to powinno być wysyłane oddzielnym kanałem telekomunikacyjnym.

B. OSOBY ODPOWIEDZIALNE ZA BEZPIECZEŃSTWO INFORMACJI I PRZETWARZANIE DANYCH OSOBOWYCH ROLE I ODPOWIEDZIALNOŚCI

1. FUNKCJE/ODPOWIEDZIALNOŚCI ZWIĄZANE Z REALIZACJĄ POSTANOWIEŃ POLITYKI OCHRONY DANYCH

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

1) Administrator Danych (ADO)- ZESPÓŁ SZKÓŁ W DZWOLI,
2) Inspektor Ochrony Danych,
3) Administrator Systemów Informatycznych,
4) Osoby upoważnione do przetwarzania danych osobowych.

1.1. ADMINISTRATOR DANYCH

1. Administrator Danych wyznacza:
   1) Inspektora Ochrony Danych (IOD),
   2) Administratora Systemów Informatycznych.
2. Administrator Danych jest odpowiedzialny za:
   1) zapewnienie odpowiednich środków organizacyjnych i technicznych w celu zapewnienia i wykazania przetwarzania danych osobowych zgodnie z określonymi w RODO zasadami przetwarzania danych osobowych;
   2) wdrożenie odpowiednich procedur ochrony danych osobowych;
   3) jeśli uzna to za konieczne, stosowanie zatwierdzonych kodeksów postępowania lub zatwierdzonych mechanizmów certyfikacji, jako element dla stwierdzenia przestrzegania przez Administratora Danych ciążących na nim obowiązków;
   4) zapewnienie środków umożliwiających prawidłowa realizację praw osób, których dane dotyczą,
   5) prowadzenie rejestru czynności przetwarzania danych osobowych;
   6) prowadzenie rejestru kategorii przetwarzania dokonywanych w imieniu innego administratora,
   7) współpracę z organem nadzorczym w ramach wykonywania przez niego swoich zadań;
   8) wdrożenie odpowiednich środków organizacyjnych i technicznych, aby zapewnić stopień bezpieczeństwa odpowiadający istniejącemu ryzyku naruszenia praw lub wolności osób, których dane dotyczą;

9) zgłaszanie naruszenia ochrony danych osobowych właściwemu organowi nadzorczemu, a w przypadku, gdy zajdą ku temu odpowiednie przesłanki, również osobie, której dane dotyczą;
10) dokumentowanie wszelkich naruszeń ochrony danych osobowych, w tym okoliczności naruszenia, jego skutków oraz podjętych działań zaradczych;
11) zapewnienie odpowiednich środków w celu dokonania oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych w sytuacji, jeżeli dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, w tym, jeżeli zajdą ku temu odpowiednie przesłanki, konsultację z organem nadzorczym;
12) nadawanie upoważnień do przetwarzania danych osobowych oraz prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;
13) zapewnienie legalności przekazywania danych osobowych do podmiotów trzecich.

3. Administrator Danych w stosunku do IOD jest odpowiedzialny za:
   1) zapewnienie, że jest on właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych;
   2) wspieranie IOD 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;
   3) zagwarantowanie by IOD wykonywał swoją funkcję niezależnie, nie działał pod wpływem presji i nie otrzymywał instrukcji dotyczących wykonywania swoich zadań;
   4) publikację danych kontaktowych IOD oraz zawiadomienie o nich organu nadzorczego.

1.2. INSPEKTOR OCHRONY DANYCH

1. Funkcję IOD pełni osoba wyznaczona przez Administratora Danych.
2. Inspektor Ochrony Danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności powinien:
   1) posiadać fachową wiedzę na temat prawa i praktyk w dziedzinie ochrony danych osobowych;
   2) posiadać umiejętność wypełniania zadań określonych w RODO;
   3) dysponować wiedzą na temat procedur administracyjnych i funkcjonowania jednostki.
3. Administrator Danych po wyznaczeniu Inspektora Ochrony Danych zawiadamia o tym fakcie Prezesa Urzędu Ochrony Danych Osobowych w terminie 14 dni od dnia wyznaczenia.
4. Zmiana danych Inspektora bądź jego odwołanie następuje z zachowaniem terminu 14 dni.
5. Administrator Danych udostępnia na swojej stronie internetowej dane kontaktowe Inspektora tj.: imię i nazwisko oraz dane kontaktowe (nr telefonu lub adres e-mail).
6. Inspektor Ochrony Danych Pełni funkcję opiniodawczo- doradczo- weryfikacyjną i jest odpowiedzialny za:
   1) informowanie Administratora oraz osób upoważnionych do przetwarzania danych osobowych o obowiązkach spoczywających na nich na mocy RODO oraz innych właściwych przepisów Unii lub państw członkowskich o ochronie danych osobowych oraz doradzanie w tym zakresie;
   2) monitorowanie przestrzegania RODO oraz innych właściwych przepisów Unii lub państw członkowskich o ochronie danych osobowych;
   3) monitorowanie przestrzegania wdrożonych procedur ochrony danych osobowych;
   4) opiniowanie i doradzanie w sprawach dotyczących bezpośrednio lub pośrednio ochrony danych osobowych;
   5) opiniowanie rozwiązań organizacyjnych pod kątem właściwego wdrażania systemu ochrony danych osobowych;
   6) udział, na wniosek Administratora lub z własnej inicjatywy, w weryfikacji podmiotu przed zawarciem umowy powierzenia przetwarzania danych osobowych;
   7) udział, w uzasadnionych przypadkach, w audytach i kontrolach związanych z powierzeniem przetwarzania danych osobowych podmiotom zewnętrznym;
   8) uczestniczenie w kontrolach zewnętrznych dotyczących ochrony danych osobowych;
   9) udział w postępowaniach wyjaśniających w zakresie podejrzenia naruszenia ochrony danych osobowych, prowadzonych zgodnie z procedurą zarządzania incydentami;

10) działania zwiększające świadomość pracowników Administratora Danych w zakresie obowiązków wynikających z RODO lub przyjętych procedur;
11) szkolenia dla pracowników Administratora Danych uczestniczących w operacjach przetwarzania danych;
12) przeprowadzanie audytów w zakresie przestrzegania RODO i wdrożonych procedur ochrony danych osobowych;
13) udzielanie na żądanie zaleceń, co do oceny skutków dla ochrony danych osobowych oraz monitorowanie jej wykonania;
14) współpraca z organem nadzorczym oraz pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych;
15) pełnienie funkcji punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO.

1.3. ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH

1. Funkcję Administratora Systemów Informatycznych pełni osoba wyznaczona przez Administratora Danych.
2. Administrator Systemów Informatycznych odpowiedzialny jest za zarządzanie i bieżący nadzór nad systemem informatycznym Administratora Danych.
3. Do zadań ASI należy:
   1) prowadzenie rejestru nadanych uprawnień do systemów informatycznych, przydzielanie użytkownikowi identyfikatora oraz hasła do systemu informatycznego oraz dokonywanie ewentualnych modyfikacji uprawnień;
   2) nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów;
   3) podejmowanie odpowiednich działań w przypadku wykrycia naruszenia zabezpieczeń systemu informatycznego oraz informowanie o tym fakcie Inspektora Ochrony Danych, a także współdziałanie przy usuwaniu skutków naruszenia;
   4) identyfikacja i analiza zagrożeń oraz ocena ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych;
   5) sprawowanie nadzoru nad kopiami zapasowymi;
   6) inicjowanie i nadzór nad wdrażaniem nowych narzędzi, procedur organizacyjnych oraz sposobów zarządzania systemami informatycznymi, które mają doprowadzić do wzmocnienia bezpieczeństwa przy przetwarzaniu danych osobowych;
   7) podejmowanie innych czynności w zakresie zabezpieczenia przetwarzania danych w systemach informatycznych;
   8) ścisła współpraca z IOD w zakresie bezpieczeństwa i zasad przetwarzania danych osobowych w systemach informatycznych.

1.4. OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator Danych realizując Politykę, w zakresie udostępniania danych osobowych w ramach własnej (wewnętrznej) struktury, zezwala na ich przetwarzanie w systemie informatycznym lub w wersji papierowej wyłącznie osobom, które uzyskały uprzednie, stosowne upoważnienie do przetwarzania danych osobowych.
2. Każdy pracownik jest obowiązany do należytego przestrzegania zasad ochrony danych osobowych określonych w RODO oraz w Polityce, w szczególności do:
   1) przetwarzania danych osobowych w zakresie swojego upoważnienia i zgodnie z celami przetwarzania;
   2) przestrzegania zasad bezpieczeństwa dotyczących eksploatacji systemów teleinformatycznych, a także korzystania z systemów teleinformatycznych służących do przetwarzania danych osobowych wyłącznie zgodnie z ich przeznaczeniem i w zakresie swoich zadań, a także do ochrony przed nieupoważnionym dostępem do tych systemów;
   3) informowania przełożonego o wszelkich zauważonych nieprawidłowościach i zdarzeniach skutkujących lub mogących skutkować obniżeniem poziomu ochrony danych osobowych;
   4) zgłaszania zdarzeń mogących stanowić naruszenie ochrony danych osobowych, zgodnie z procedurą zarządzania incydentami i uczestniczenia w czynnościach wyjaśniających;
   5) zapewnienia poufności przetwarzanych danych osobowych oraz poufności sposobów zabezpieczenia danych osobowych, w trakcie wykonywania powierzonych zadań i po ich zakończeniu, w tym zapewnienia ochrony danych osobowych przed nieuprawnionym dostępem (w tym fizycznym), nieuzasadnioną modyfikacją, zniszczeniem, ujawnieniem lub pozyskaniem danych;
   6) zapoznania się z Polityką i potwierdzenia tego w formie pisemnej
   7) stosowania następujących zasad bezpieczeństwa:
      a) czystego biurka– podczas nieobecności pracownika na stanowisku pracy, także w przypadku krótkotrwałego opuszczenia pomieszczenia, dokumenty i informatyczne nośniki danych zawierające informacje prawnie chronione lub przeznaczone do użytku wewnętrznego należy zabezpieczyć przed dostępem osób postronnych i nieupoważnionych. Po zakończeniu pracy wszystkie dokumenty i informatyczne nośniki przechowuje się w miarę możliwości organizacyjno-technicznych w nieprzeszklonych, zamykanych na klucz meblach biurowych, zamykanych na klucz lub kod szafach metalowych, przeznaczonych do tego pomieszczeniach zamykanych na klucz lub wyposażonych w system kontroli dostępu;

b) czystego ekranu– na czas nieobecności pracownika dostęp do komputera jest blokowany, a po zakończeniu pracy komputer jest wyłączany, chyba że dany komputer musi pracować w trybie ciągłym– w szczególności dotyczy to serwera obsługującego systemy alarmowe, komputerów administratorów, serwerów do monitoringu. W czasie obecności pracownika monitor jest ustawiony tak, aby nie pozwalał na zapoznawanie się z wyświetlanymi treściami przez osoby postronne, nieupoważnione;

c) czystego kosza– dokumenty papierowe, z wyjątkiem materiałów zawierających informacje publicznie dostępne, w tym promocyjno-informacyjne, muszą być niszczone w sposób uniemożliwiający ich odczytanie lub odtworzenie. W celu zniszczenia dokumentów papierowych zawierających informacje wrażliwe i prawnie chronione należy korzystać z udostępnionych niszczarek o odpowiedniej klasie niszczenia, adekwatnej do informacji oraz danych utrwalonych na niszczonych dokumentach;

d) czystej tablicy– po zakończonym spotkaniu należy uprzątnąć wszystkie materiały oraz wyczyścić tablice oraz flipchart;

e) czystych drukarek– w przypadku drukowania dokumentów z użyciem ogólnodostępnej drukarki drukowane informacje są zabierane z drukarek niezwłocznie po wydrukowaniu. W przypadku nieudanej próby wydrukowania użytkownik ma obowiązek skontaktować się z osobą odpowiedzialną za eksploatację urządzenia, jeżeli zachodzi podejrzenie, iż wydruk zostanie wydrukowany bez nadzoru;

f) zamkniętego pomieszczenia– niedopuszczalne jest pozostawienie pod nieobecność pracownika niezabezpieczonego pomieszczenia służbowego, zarówno w godzinach pracy, jak i po jej zakończeniu. Na zakończenie dnia pracy ostatnia wychodząc z pomieszczenia osoba jest obowiązana zamknąć wszystkie okna i drzwi oraz zabezpieczyć klucze do pomieszczenia;

g) zgłaszania incydentów bezpieczeństwa informacji i naruszeń ochrony danych osobowych– każdy użytkownik ma obowiązek niezwłocznie zgłosić wystąpienie lub podejrzenie wystąpienia incydentu lub naruszenia mającego lub mogącego mieć wpływ na bezpieczeństwo informacji, w tym danych osobowych w Urzędzie;

3. Upoważnienie do przetwarzania danych osobowych nadawane jest po przeprowadzeniu szkolenia lub zaznajomieniu w innej formie, osoby upoważnianej z zasadami ochrony danych osobowych obowiązującymi w strukturze Administratora Danych.

4. Upoważnienie przygotowuje wyznaczony pracownik, po uprzednim poinformowaniu przez Administratora Danych.

5. Upoważnienia wydawane są w formie pisemnej albo elektronicznej.

6. Upoważnienie wydawane jest na czas określony lub nieokreślony.

7. Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia. Stosowny zapis o przyjęciu zobowiązania do zachowania w tajemnicy przetwarzanych danych osobowych zawiera upoważnienie.

8. Administrator Danych prowadzi ewidencje osób upoważnionych do przetwarzania danych osobowych.

9. Ewidencja osób upoważnionych do przetwarzania danych osobowych prowadzona jest przez osobę wyznaczoną przez Administratora Danych.

10. Ewidencja osób upoważnionych zawiera w szczególności: imię i nazwisko osoby upoważnionej, stanowisko/funkcję, datę nadania i datę ustania upoważnienia, zakres upoważnienia.

11. Nie rzadziej niż raz do roku Administrator Danych dokonuje analizy poprawności prowadzonej ewidencji, a także analizy wydanych upoważnień pod kątem ich aktualności oraz prawidłowości ich zakresu. W przypadku stwierdzenia nieaktualności lub błędów w ewidencji Administrator poprawia dane zawarte w ewidencji, a w przypadku stwierdzenia braku upoważnień lub niewłaściwego ich zakresu - nadaje upoważnienia lub je cofa. Przeprowadzenie analizy i jej wyników Administrator odpowiednio odnotowuje. Analiza obejmuje także przegląd uprawnień w systemach teleinformatycznych służących do przetwarzania danych osobowych.

12. Wzór oświadczenia o znajomości Polityki ochrony danych oraz zachowaniu przetwarzanych danych w tajemnicy stanowi załącznik nr 4 do Polityki.

13. Wzór upoważnienia do przetwarzania danych stanowi załącznik nr 5 do Polityki.

14. Wzór ewidencji osób upoważnionych do przetwarzania danych stanowi załącznik nr 6 do Polityki.

C. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

1. OGÓLNE ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator Danych- działa wyłącznie w granicach określonych przepisami prawa i przetwarza dane osobowe osób fizycznych zgodnie z ogólnymi zasadami określonymi w art. 5 RODO.

2. Dane osobowe przetwarza się:

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

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

   3) w sposób przejrzysty dla osób, których dane dotyczą (zasada przejrzystości);

   4) w konkretnych, wyraźnych i prawnie uzasadnionych celach (zasada ograniczenia celu);

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

   6) przy uwzględnieniu ich prawidłowości i ewentualnego uaktualniania (zasada prawidłowości);

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

   8) w sposób zapewniający odpowiednie bezpieczeństwo (integralność i poufność).

3. Dane osobowe (tzw. zwykłe) mogą być przetwarzane, o ile spełniony jest jeden z warunków zawartych w art. 6 ust. 1 RODO:

   1) przetwarzanie jest niezbędne do wypełnienia przez Administratora obowiązku wynikającego z przepisów (art. 6 ust. 1 lit. c RODO);

   2) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi (art. 6 ust. 1 lit. e RODO - stosowany, kiedy nie ma wyraźnego przepisu prawa, ale może być wykazany interes publiczny lub sprawowanie władzy publicznej w odpowiednim zakresie, wynikającym z przepisów);

   3) przetwarzanie jest niezbędne do wykonania umowy z osobą, która jest jej stroną, lub w celu zawarcia takiej umowy (art. 6 ust. 1 lit. b RODO);

4) przetwarzanie jest niezbędne do celów, które wynikają z prawnie uzasadnionych interesów realizowanych przez Administratora (art. 6 ust. 1 lit. f RODO - przesłanki tej nie można stosować, kiedy Administrator wykonuje zadania organu);

5) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej (art. 6 ust. 1 lit. d RODO).

4. Dane szczególnych kategorii (tzw. dane wrażliwe) mogą być przetwarzane, o ile spełniony jest jeden z warunków zawartych w art. 9 ust. 2 RODO:

   1) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez Administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalne (art. 9 ust. 2 lit. b RODO);

   2) przetwarzanie jest niezbędne dla ochrony życia lub zdrowia lub interesów osoby, której dane dotyczą lub innej osoby (art. 9 ust. 2 lit. c RODO), przy czym dodatkowo musi być spełniony warunek, że osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody);

   3) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, na podstawie przepisów prawa (art. 9 ust. 2 lit. h RODO);

   4) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym i odbywa się na podstawie przepisów spełniających warunki określone w art. 9 ust. 2 lit. g RODO);

   5) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń (art. 9 ust. 2 lit. f RODO);

   6) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, na podstawie przepisów prawa (art. 9 ust. 2 lit. i RODO);

   7) dane zostały upublicznione przez osobę, której dotyczą (art. 9 ust. 2 lit. e RODO);

   8) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych (art. 9 ust. 2 lit. j RODO);

5. W przypadku, gdy przetwarzanie danych osobowych (zwykłych lub wrażliwych) nie może być oparte na jednej z przesłanek legalności, określonych w ust. 1 lub 2, podstawą przetwarzania danych osobowych może być zgoda osoby, której dane dotyczą (art. 6 ust. 1 lit. a RODO lub art. 9 ust. 2 lit. a RODO).

6. Każdy pracownik odbierający zgodę osoby, której dane dotyczą, tworzy warunki, aby zgoda była udzielona dobrowolnie, świadomie i wobec konkretnego celu, a także w przypadku, kiedy zgoda nie jest składana na piśmie, dokumentuje, w szczególności adnotacją, czy była złożona przez oświadczenie czy wyraźne działanie osoby, której dane dotyczą, potwierdzające przyzwolenie na przetwarzanie dotyczących jej danych osobowych. Zgoda na przetwarzanie danych wrażliwych musi być wyrażona na piśmie.
7. Administrator Danych przetwarzając dane osobowe na podstawie zgody, zapewnia- przed wyrażeniem zgody przez osobę, której dane dotyczą - poinformowanie jej, że zgoda może być cofnięta w każdym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.
8. W przypadku cofnięcia zgody przez osobę, której dane dotyczą, Administrator Danych niezwłocznie podejmuje czynności zmierzające do zaprzestania dalszego przetwarzania danych osobowych, dokonywanego w oparciu o przesłankę zgody.
9. W przypadku przetwarzania danych na podstawie zgody osoby, której dane dotyczą, należy stosować oświadczenie o wyrażeniu zgody na przetwarzanie danych osobowych, którego wzór stanowi zał. nr 7 do niniejszej Polityki (wzór służy do konstruowania szczegółowych zgód na przetwarzanie danych osobowych), a wzór oświadczenia o wycofaniu zgody na przetwarzanie danych osobowych znajduje się w załączniku nr 8.

2. ZASADA OCHRONY DANYCH OSOBOWYCH W FAZIE PROJEKTOWANIA ORAZ DOMYŚLNA OCHRONA DANYCH OSOBOWYCH

1. Administrator Danych na etapie projektowania i opracowywania sposobów przetwarzania danych, a ponadto także na każdym kolejnym etapie przetwarzania, ma obowiązek uwzględniać obowiązujące zasady ochrony danych osobowych.
2. Administrator Danych wdraża odpowiednie środki techniczne i organizacyjne, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, nadania przetwarzaniu danych niezbędnych zabezpieczeń oraz zapewnieniu ochrony praw osób, których dane dotyczą.
3. Przy wyborze środków należy uwzględnić czynniki takie jak:
   1) stan wiedzy technicznej;
   2) koszt wdrażania;
   3) charakter, zakres, kontekst i cele przetwarzania danych;
   4) ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania.
4. Środki służące realizacji tego obowiązku mogą polegać m. in. na:
   1) minimalizacji przetwarzania danych osobowych;
   2) jak najszybszej pseudonimizacji danych osobowych;
   3) przejrzystości co do funkcji i przetwarzania danych osobowych;
   4) umożliwienia osobie, której dane dotyczą, monitorowania przetwarzania danych;
   5) umożliwienia Administratorowi tworzenia i doskonalenia zabezpieczeń.
5. Administrator Danych w przypadku zakupu środków technicznych lub modernizacji i modyfikacji powinien zasięgnąć opinii niezależnego audytora strony trzeciej działającego na rzecz i w imieniu ADO.
6. Administrator Danych wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia określonego 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, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.

7. W pierwszej kolejności, Administrator Danych rozważa, czy cel jakiemu ma służyć projektowane rozwiązane jest możliwy do osiągnięcia bez konieczności przetwarzania danych osobowych. Jeśli tak, należy wybrać takie rozwiązanie.

3. ANONIMIZACJA

1. W przypadku, gdy nie ma już potrzeby dalszego przetwarzania danych osobowych, a dane są potrzebne do prowadzenia prac analitycznych, statystycznych lub testowych, Administrator Danych zapewnia anonimizację danych osobowych, polegającą na nieodwracalnym ich usunięciu lub takiej ich modyfikacji, która uniemożliwi identyfikację osoby fizycznej.

2. Za prawidłową anonimizację dokumentu, wykonaną w odpowiednim momencie przetwarzania danych osobowych, w szczególności przed ich udostępnieniem, niezależnie od postaci danych, elektronicznej czy papierowej, jest odpowiedzialny pracownik prowadzący sprawę oraz jego bezpośredni przełożony.

4. PSEUDONIMIZACJA

1. W celu zabezpieczenia danych osobowych, które będą potrzebne do późniejszego wykorzystania, przed nieuprawnionym ujawnieniem, Administrator Danych stosuje pseudonimizację, polegającą na przetworzeniu danych osobowych w taki sposób, by nie była możliwa identyfikacja osoby fizycznej, bez użycia dodatkowych informacji (np. klucza pseudonimizacyjnego). Te dodatkowe informacje Administrator Danych danych przechowuje osobno, zabezpieczając je technicznie i organizacyjnie przed nieuprawnionym użyciem mającym na celu odwrócenia procesu pseudonimizacji.

5. POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator Danych realizując Politykę ochrony danych dopuszcza, by dane osobowe, których jest administratorem były przetwarzane poza własnymi strukturami organizacyjnymi.
2. W przypadku wystąpienia potrzeby zapewnienia podmiotowi zewnętrznemu dostępu do danych osobowych, jest wymagane uprzednie:
   1) zawarcie odrębnej umowy powierzenia przetwarzania danych osobowych, albo
   2) zawarcie stosownych regulacji dotyczących powierzenia przetwarzania danych osobowych w umowie podstawowej, albo
   3) zawarcie stosownych regulacji dotyczących powierzenia przetwarzania danych osobowych w innym instrumencie prawnym
3. Administrator Danych wdraża stosowanie wzorców umów powierzenia przetwarzania danych osobowych.
4. Dopuszcza się stosowanie wzorców umów dostarczonych przez kontrahentów, pod warunkiem ich udokumentowanej akceptacji przez najwyższe kierownictwo oraz Inspektora Ochrony Danych.
5. Zabrania się powierzania przetwarzania danych osobowych bez odpowiedniej umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego, zgodnego z art. 28 RODO.
6. Podstawowym warunkiem dopuszczalności powierzenia przetwarzania danych w imieniu administratora jest poddanie planowanego outsourcingu analizie, która powinna zapewnić, że wybór podmiotu przetwarzającego został uzależniony od zapewnienia wystarczających gwarancji ochrony danych.
7. Zawierana przez Administratora Danych umowa powierzenia przetwarzania danych osobowych musi być zgodna z postanowieniami art. 28 RODO, tj. w szczególności określać:
   1) przedmiot powierzenia;
   2) czas trwania powierzenia;
   3) charakter i cel przetwarzania;
   4) rodzaj powierzanych danych osobowych;
   5) kategorie osób, których dane dotyczą;
   6) warunki podpowierzenia przetwarzania danych;
   7) obowiązki i prawa Administratora Danych;

8) obowiązki podmiotu przetwarzającego.

8. Umowa powierzenia może zostać zawarta w formie pisemnej, w tym elektronicznej.

9. W przypadku, gdy elementy powierzenia przetwarzania danych wskazane w pkt 6 znajdują się już w zawartej z danym podmiotem umowie głównej/ bazowej, nie ma konieczności sporządzania dodatkowej umowy powierzenia przetwarzania danych osobowych.

10. Administrator Danych przed planowanym rozpoczęciem współpracy z podmiotem przetwarzającym, jest zobowiązany poinformować o tym IOD oraz skonsultować z nim postanowienia zawieranej umowy w zakresie powierzenia przetwarzania danych osobowych. Powierzenie przetwarzania danych może odbyć się wyłącznie na podstawie postanowień zaakceptowanych przez IOD.

11. Każdorazowe dokonanie powierzenia danych osobowych musi zostać obligatoryjnie odnotowane w ewidencji podmiotów, którym Administrator powierzył przetwarzanie Danych.

12. Administrator Danych ma prawo kontroli podmiotów przetwarzających, którym powierzył przetwarzanie danych osobowych.

13. Administrator Danych w zakresie prowadzonej przez siebie działalności może przetwarzać również dane osobowe powierzone przez podmioty, na rzecz których świadczy usługi. Przyjęcie danych w powierzenie przez Administratora Danych musi zostać obligatoryjnie odnotowane w rejestrze kategorii czynności przetwarzania danych osobowych.

14. Administrator przed powierzeniem przetwarzania danych osobowych zobligowany jest do uzyskania informacji o stosowanych środkach technicznych i organizacyjnych przez podmiot przetwarzający za pomocą listy kontrolnej procesora stanowiącej zał. nr 9 do niniejszej Polityki.

15. Administrator przyjął minimalne wymagania co do treści umowy powierzenia przetwarzania danych, której wzór stanowi zał. nr 10.

16. Administrator po zawarciu każdej umowy powierzenia odnotowuje ten fakt w rejestrze zawartych umów powierzenia, którego wzór stanowi zał. nr 11.

6. UDOSTĘPNIENIE DANYCH OSOBOWYCH

1. Administrator Danych realizując Politykę dopuszcza, by dane osobowe, których jest administratorem były przekazywane innym administratorom w formie udostępnienia danych.
2. Administrator Danych udostępnia dane osobowe innym podmiotom lub osobom wyłącznie na podstawie przepisów prawa.:
    1) na wniosek osoby, której dane dotyczą;
    2) za wyraźną zgodą podmiotu, którego dane dotyczą;
    3) na wniosek podmiotu uprawnionego do otrzymywania danych osobowych (np.: Policji, Prokuraturze);
    4) na podstawie umowy z innym podmiotem, w ramach której istnieje konieczność udostępnienia danych.
3. W przypadku, , kiedy wniosek o udostępnienie danych nie zawiera podstawy prawnej lub zawiera wadliwą podstawę prawną Administrator Danych wzywa wnioskodawcę do uzupełnienia lub odmawia udostępnienia danych osobowych. W przypadku wniosku osoby fizycznej, Administrator Danych dokłada starań w celu ustalenia właściwej podstawy prawnej udostępnienia.
4. Administrator danych weryfikuje żądanie udostępnienia danych osobowych, z którym występują organy publiczne, w szczególności pod kątem tego, czy ma formę pisemną, jest uzasadnione, ma charakter wyjątkowy i nie prowadzi do udostępniania wszystkich danych osobowych zawartych w określonym zbiorze lub systemie oraz czy nie prowadzi do łączenia zbiorów danych osobowych.
5. Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystywać wyłącznie w celu dla którego zostały zebrane.
6. Informacje zawierające dane osobowe Administrator Danych przekazuje uprawnionym podmiotom lub osobom w następujący sposób:
    1) w postaci papierowej - przesyłką pocztową;
    2) w postaci elektronicznej - za pomocą teletransmisji danych, w postaci zabezpieczonej;
    3) w inny sposób - określony konkretnym wymogiem prawnym, umową lub porozumieniem.
7. W przypadku wpływu wniosku pochodzącego od osoby, której dane dotyczą w sprawie żądania udzielenia informacji na temat przetwarzania jej danych osobowych, odpowiedź na przedmiotowy wniosek następuje w terminie 30 dni od daty jego otrzymania.

7. PRZEKAZYWANIE DANYCH OSOBOWYCH DO PAŃSTW TRZECICH LUB ORGANIZACJI MIĘDZYNARODOWEJ

1. Przekazywanie danych, których administratorem jest Administrator Danych do państw trzecich lub organizacji międzynarodowych, może nastąpić zgodnie z art. 44–46 RODO.
2. W przypadku niespełnienia warunków, o których mowa w ust. 1, przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić wyłącznie zgodnie z art. 49 RODO.
3. Administrator Danych przed planowanym przekazaniem danych do państwa trzeciego lub organizacji międzynarodowej, jest zobowiązany poinformować o tym IOD oraz skonsultować z nim warunki przekazania tych danych. Przekazanie danych może odbyć się wyłącznie na podstawie warunków i postanowień zaakceptowanych przez IOD.

8. REALIZACJA PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ

1. Administrator Danych uwzględnia w zachodzących w jego strukturze procesach przetwarzania danych osobowych, procedury i zasady ułatwiające osobie, której dane dotyczą, wykonywanie praw przysługujących jej na mocy przepisów RODO.
2. Osoba, której dane dotyczą ma prawo do:
   1) wycofania wyrażonej zgody (art. 7 ust. 3 RODO);
   2) dostępu do swoich danych (art. 15 RODO);
   3) sprostowania danych (art. 16 RODO);
   4) usunięcia danych (prawo do bycia zapomnianym) (art. 17 RODO);
   5) ograniczenia przetwarzania (art. 18 RODO);
   6) przenoszenia danych (art. 20 RODO);
   7) wniesienia sprzeciwu (art. 21 RODO);
   8) niepodlegania decyzjom opartym na zautomatyzowanym przetwarzaniu (art. 22 RODO).
3. Każda osoba, której dane dotyczą, ma prawo skorzystać z niniejszych praw poprzez złożenie wniosku do Administratora Danych.
4. Przedmiotowy wniosek zostaje dekretowany do Inspektora Ochrony Danych, który analizuje treść dokumentu, po której sporządza notatkę i w formie pisemnej przedstawia propozycję wykonania czynności Administratorowi Danych wraz z przedmiotowym wnioskiem.
5. Wzór ewidencji żądań od podmiotów danych osobowych o których mowa w art.15-21 RODO stanowi załącznik nr 12 do Polityki.
6. Procedura realizacji praw osób, których dane dotyczą stanowi zał. nr 13 do Polityki.

9. REALIZACJA OBOWIĄZKÓW INFORMACYJNYCH

1. Administrator realizuje obowiązek informacyjny w stosunku do osób fizycznych od których bezpośrednio są zbierane dane osobowe zgodnie z art. 13 ust.1 i 2 RODO oraz w stosunku do osób, których dane zostały zebrane z innego źródła aniżeli bezpośrednio od osoby, której dane dotyczą zgodnie z art. 14 ust. 1 i 2 RODO.
2. Administrator Danych odpowiada za realizację obowiązku informacyjnego zgodnie z art. 13 ust. 1 i 2 RODO, chyba że osoba, której dane dotyczą dysponuje już wszystkimi informacjami.
3. Obowiązek informacyjny jest realizowany przez udostępnienie w odpowiedni sposób klauzuli informacyjnej.
4. Administrator Danych może realizować obowiązki informacyjne przez umieszczenie klauzul informacyjnych w miejscu publicznie dostępnym w siedzibie oraz udostępnienie w Biuletynie Informacji Publicznej na stronie podmiotowej tego organu, pod warunkiem przekazania osobie podczas pozyskiwania danych osobowych informacji o miejscu udostępnienia informacji o przetwarzaniu danych osobowych.
5. Administrator podczas pozyskiwania danych od osoby, której dane dotyczą jest zobowiązany poinformować tę osobę o:
    1) swojej tożsamości i danych kontaktowych;
    2) danych kontaktowych Inspektora Ochrony Danych;
    3) celu i podstawie prawnej przetwarzania tych danych osobowych;
    4) prawnie uzasadnionym interesie realizowanym przez Administratora Danych lub stronę trzecią;
    5) odbiorcach danych lub kategorii odbiorców;
    6) okresie, przez który te dane będą przechowywane, a gdy nie jest to możliwe, kryteria ustalenia takiego okresu;
    7) prawie do żądania od Administratora:
        a) dostępu do danych osobowych osoby, której te dane dotyczą,
        b) do sprostowania jej danych osobowych,
        c) do usunięcia jej danych osobowych,
        d) do ograniczenia przetwarzania jej danych osobowych,
        e) do wniesienia sprzeciwu wobec przetwarzania jej danych osobowych,
        f) do przenoszenia danych;
    8) prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem jeżeli przetwarzanie odbywa się na podstawie zgody;
    9) prawie wniesienia skargi do organu nadzorczego;

10) właściwości: czy podanie danych 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 nie podania tych danych;
11) zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję Europejską odpowiedniego stopnia ochrony lub w przypadku przekazania, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych;
12) zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą;

5. Administrator danych w przypadku zbierania danych nie od osoby, której dane dotyczą, osobę tę należy poinformować dodatkowo o kategorii i źródle pochodzenia danych osobowych.
6. Administrator danych prowadzi ewidencję stosowanych klauzul informacyjnych. Wzór ewidencji stosowanych klauzul informacyjnych stanowi załącznik nr 14 do Polityki.

10. ZARZĄDZANIE RYZYKIEM W ZAKRESIE OCHRONY DANYCH OSOBOWYCH

1. Ocena ryzyka jest prowadzona okresowo, zgodnie z procedurą oceny ryzyka, dla poszczególnych czynności przetwarzania danych osobowych oraz jest na bieżąco aktualizowana.
2. Inspektor ochrony Danych we współpracy z Administratorem analizuje możliwe sytuacje i naruszenia ochrony danych osobowych uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, zwane dalej ,, analizami ryzyka''.
3. Inspektor ochrony Danych we współpracy z Administratorem przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub uch kategorii.
4. Analiza ryzyka powinna zapewniać:
    1) zidentyfikowanie ryzyka;
    2) oszacowanie ryzyka z punktu widzenia następstw dla działalności jednostki oraz prawdopodobieństwa wystąpienia takiego ryzyka;
    3) informowanie o następstwach wystąpienia ryzyka;
    4) ustanowienie priorytetów w postępowaniu z ryzykiem;
    5) regularne monitorowanie i przegląd różnych typów ryzyka oraz procesu zarządzania ryzykiem;
    6) zbieranie informacji w celu doskonalenia podejścia do zarządzania ryzykiem.
5. Administrator dokumentuje wykonaną analizę ryzyka w postaci raportu.
6. Administrator dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych w przypadkach, w których zgodnie z analizą ryzyka, ryzyko naruszenia praw i wolności osób jest wysokie oraz w każdym przypadku, gdy wymagają tego obowiązujące przepisy prawa i wytyczne Prezesa Urzędu Ochrony Danych Osobowych.

11. OCENA SKUTKÓW DLA OCHRONY DANYCH OSOBOWYCH

1. Ocenę skutków dla ochrony danych osobowych przeprowadza się dla:
   1) operacji przetwarzania danych osobowych, dla których określono wysokie ryzyko naruszenia praw lub wolności osób fizycznych;
   2) operacji wymienionych przez Prezesa UODO w wykazie rodzajów operacji przetwarzania;
   3) podlegających wymogowi dokonania oceny skutków dla ochrony danych osobowych.
2. Przeprowadzenie oceny skutków dla ochrony danych osobowych ma na celu ustalenie, czy po uwzględnieniu ryzyk oraz planowanych zabezpieczeń, ryzyko naruszenia praw lub wolności osób fizycznych pozostaje wysokie.
3. W przypadku wykazania wysokiego ryzyka naruszenia praw lub wolności osób fizycznych, mimo zastosowanych zabezpieczeń, przed rozpoczęciem przetwarzania danych osobowych, Administrator Danych, we współpracy z IOD, przeprowadza uprzednie konsultacje z Prezesem UODO, zgodnie z art. 36 RODO.

12. POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH ORAZ INNYCH ZDARZEŃ ZWIĄZANYCH Z BEZPIECZEŃSTWEM DANYCH OSOBOWYCH

1. Osobami odpowiedzialnymi za bezpieczeństwo danych osobowych, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do pomieszczeń oraz systemów, w których przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia incydentów ochrony danych osobowych, jest: Administrator Danych, IOD oraz ASI (w odniesieniu do danych przetwarzanych w systemach informatycznych).
2. Każdy jest zobowiązany zawiadomić o przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych, niezależnie od tego, czy miało ono miejsce w systemie teleinformatycznym służącym do przetwarzania danych osobowych, czy poza systemem, lub o innym zdarzeniu wskazującym na naruszenie ochrony danych osobowych lub mogącym skutkować obniżeniem poziomu ochrony danych osobowych.
3. Sposób i tryb zgłaszania naruszeń oraz proces obsługi naruszeń ochrony danych osobowych uregulowany jest w procedurze która stanowi załącznik nr 15 do Polityki.

13. ODPOWIEDZIALNOŚĆ (SANKCJE)

Odpowiedzialność karną, dyscyplinarną lub służbową za naruszenie przepisów dotyczących ochrony danych osobowych określają przepisy odrębne.

14. AUDYT ZGODNOŚCI PRZETWARZANIA DANYCH

1. W celu zapewnienia przestrzegania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz procedurami wdrożonymi w strukturze Administratora Danych, Inspektor Ochrony Danych przeprowadza Audyt zgodności przetwarzania danych osobowych w tym:
   1) sprawdzenie prawidłowości i aktualności dokumentacji z zakresu ochrony danych osobowych;
   2) sprawdzenie przestrzegania zasad i procedur określonych w dokumentacji ochrony danych osobowych;
   3) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych.
2. Audyt przeprowadzany jest okresowo zgodnie z opracowanym przez IOD planie audytów.
3. IOD przygotowuje plan audytów na okres nie dłuższy niż rok.
4. Plan audytów IOD przedstawia Administratorowi Danych nie później niż na dwa tygodnie przed dniem rozpoczęcia okresu objętego planem.
5. W sytuacji powzięcia wiadomości o naruszeniu ochrony danych osobowych lub uzasadnionego podejrzenia wystąpienia takiego naruszenia Inspektor Ochrony Danych przeprowadza audyt nieobjęty planem sprawdzeń (tzw. sprawdzenie doraźne).
6. W toku audytu IOD dokonuje i dokumentuje czynności, w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz do opracowania sprawozdania.
7. Po zakończeniu audytu, IOD przygotowuje dla Administratora Danych, Raport z audyty zgodności przetwarzania danych osobowych. Raport sporządzany jest w postaci elektronicznej albo w postaci papierowej.
8. IOD przekazuje Administratorowi Danych Raport z audyty zgodności przetwarzania danych osobowych nie później niż w terminie 1 miesiąca od zakończenia audytu.
9. Obowiązki określone w ust. 1-8 IOD realizuje we współpracy z Administratorem Systemów Informatycznych oraz Administratorem Danych.

15. DZIAŁANIA ZWIĘKSZAJĄCE ŚWIADOMOŚĆ OBOWIĄZKÓW DOTYCZĄCYCH OCHRONY DANYCH OSOBOWYCH, SZKOLENIA Z OCHRONY DANYCH OSOBOWYCH

1. Szkolenia z zakresu ochrony danych osobowych są prowadzone przez IOD i inne wyznaczone osoby, w formie szkoleń bezpośrednich, z wykorzystaniem technologii informatycznych, w szczególności w formie e-learningu lub w innych formach adekwatnych do celów szkolenia. Dopuszczalne jest również samokształcenie kierowane pod warunkiem zapewnienia możliwości konsultacji niejasnych zagadnień.

2. Zakres, formy i tematykę szkoleń ustala IOD lub inne osoby odpowiedzialne za szkolenie pracowników, w porozumieniu z IOD.

3. Szkolenia przeprowadzane są dla nowo przyjętych pracowników, a także według potrzeb. W ramach szkolenia nowo przyjęty pracownik jest zobowiązany do zapoznania się z przepisami prawa w zakresie ochrony danych osobowych.

4. Dodatkowo szkolenia są przeprowadzane w przypadku każdej istotnej zmiany zasad lub przepisów dotyczących ochrony danych osobowych.

5. Szkolenia dokumentowane są w formie list szkoleniowych oraz certyfikatów.

16. PRZEGLĄD, OCENA I AKTUALIZACJA/ DOSKONALENIE POLITYKI OCHRONY DANYCH OSOBOWYCH ORAZ POWIĄZANYCH DOKUMENTÓW

1. Polityka ochrony danych wymaga okresowego przeglądu pod kątem jej adekwatności, nie rzadziej niż raz do roku.
2. Przeglądu Polityki dokonuje Inspektor Ochrony Danych we współpracy z Administratorem Danych.
3. Przegląd powinien obejmować, w szczególności ocenę adekwatności Polityki do:
   1) procesów funkcjonujących w strukturach Administratora Danych;
   2) obowiązujących przepisów prawa odnoszących się do ochrony danych osobowych, którym podlega Administrator Danych.
4. Inspektor Ochrony Danych we współpracy z Administratorem Danych wykonuje przegląd Polityki niezwłocznie w przypadku gdy:
   1) zmianie ulegają przepisy prawa będące źródłem wskazanych w Polityce obowiązków;

2) zaistnieją istotne zmiany faktyczne w ramach struktury Administratora Danych;

3) dojdzie do naruszenia ochrony danych;

4) pojawią się nowe i istotne rodzaje ryzyka.

5. Jeżeli w wyniku przeglądu Polityki stwierdzona zostanie konieczność aktualizacji jej zapisów, Inspektor Ochrony Danych dokonuje aktualizacji Polityki w wymaganym zakresie.

6. Każdy przegląd udokumentowany jest raportem z przeglądu, oceny i aktualizacji/doskonalenia Polityki.

7. Po dokonanym przeglądzie i stwierdzeniu konieczności dokonania zmian w Polityce Inspektor Ochrony Danych przedstawia Administratorowi Danych propozycję zmian.

8. W celu zapewnienia właściwego wywiązywania się przez Administratora z obowiązku wynikającego z przepisów art. 32 RODO zostaje wprowadzona procedura regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mająca zapewnić bezpieczeństwo przetwarzania która stanowi załącznik nr 16 do niniejszej Polityki.

17. ZAŁĄCZNIKI POWIĄZANE Z PODO

Lp.	Wskazanie dokumentu
1.	Wykaz obszarów przetwarzania wraz z opisem środków technicznych stosowanych do zabezpieczenia danych osobowych
2.	Wzór rejestru czynności przetwarzania
3.	Wzór rejestru kategorii czynności przetwarzania
4.	Wzór oświadczenia o znajomości Polityki Bezpieczeństwa Informacji w tym Polityki ochrony danych oraz zachowaniu przetwarzanych danych w tajemnicy
5.	Wzór upoważnienia do przetwarzania danych
6.	Wzór ewidencji osób upoważnionych do przetwarzania danych
7.	Oświadczenie o wyrażeniu zgody na przetwarzanie danych osobowych
8.	Wzór oświadczenia o wycofaniu zgody na przetwarzanie danych osobowych
9.	Lista kontrolna procesora
10.	Wzór umowy powierzenia
11.	Wzór ewidencji podmiotów, którym Administrator powierzył przetwarzanie danych.
12.	Wzór ewidencji żądań od podmiotów danych osobowych o których mowa w art.15-21 RODO
13.	Procedura realizacji praw osób, których dane dotyczą.
14.	Wzór ewidencji stosowanych klauzul informacyjnych
15.	Sposób i tryb zgłaszania naruszeń oraz proces obsługi naruszeń ochrony danych osobowych
16.	Procedura regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mająca zapewnić bezpieczeństwo przetwarzania