Polityka Ochrony Danych Osobowych w Uniwersyteckim Liceum Ogólnokształcącym z Oddziałami Dwujęzycznymi w Gdańsku

1 WSTĘP

Polityka Ochrony Danych Osobowych jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora w celu spełnienia wymagań Rozporządzenia PE i RE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO).

Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z powyższym Rozporządzeniem.

2 DEFINICJE

Ilekroć w niniejszym dokumencie jest mowa o:

1) **Szkole** – rozumie się przez to Uniwersyteckie Liceum Ogólnokształcące z Oddziałami Dwujęzycznymi w Gdańsku;

2) **Administratorze** – rozumie się przez to Uniwersyteckie Liceum Ogólnokształcące z Oddziałami Dwujęzycznymi reprezentowane przez Dyrektora Szkoły;

3) **RODO** – rozumie się przez to rozporządzenie 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 (Dz. Urz. UE L 119, s. 1);

4) **polityce** – rozumie się przez to „Politykę ochrony danych osobowych przetwarzanych w Uniwersyteckim Liceum Ogólnokształcącym z Oddziałami Dwujęzycznymiw Gdańsku";

5) **IOD** w przepisach rozporządzenia – rozumie się przez to inspektora ochrony danych osobowych; (nie obowiązuje w szkole prowadzonej przez podmiot niepubliczny - zob. art 37 RODO i art. 9 ODO).

6) **ASI** – rozumie się przez to administratora systemu informatycznego, czyli pracownika odpowiedzialnego za funkcjonowanie systemu teleinformatycznego oraz stosowanie technicznych i organizacyjnych środków ochrony w tym systemie;

7) **danych osobowych** – rozumie się przez to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

8) przetwarzaniu danych osobowych – rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób

9) **zgodzie** osoby, której dane dotyczą- oznacza dowolne, dowolnie określone, konkretne, świadome i jednoznaczne wskazanie osoby, której dane dotyczą, za pomocą oświadczenia lub wyraźnego działania

potwierdzającego, wyrażającego zgodę na przetwarzanie danych osobowych z nim związanych. Zgoda musi być udokumentowana we właściwy sposób, aby ją udowodnić.
10) **podmiocie danych** - każda osoba fizyczna, która jest przedmiotem przetwarzanych danych.
11) **odbiorcy** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.
12) **podmiocie przetwarzającym** - osoba fizyczna lub prawna, organ publiczny, agencja lub jakikolwiek inny organ przetwarzający dane osobowe w imieniu administratora.
13) **anonimizacji** - przekształcenie danych osobowych w sposób uniemożliwiający przyporządkowanie poszczególnych informacji do określonej lub możliwej do zidentyfikowania osoby fizycznej.
14) **naruszeniu ochrony danych osobowych -** jest to przypadkowy lub niezgodny z prawem incydent prowadzący do zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.
15) **Szkoła jako administrator czy jako procesor**

Z uwagi na fakt, że świadczy usługi edukacyjne w wykonaniu postanowień aktu założycielskiego, statutu oraz powszechnie obowiązujących przepisów prawa, które nakładają na nie określone obowiązki, należy uznać, że w świetle art. 4 pkt 7 RODO to Uniwersyteckie Liceum Ogólnokształcące z Oddziałami Dwujęzycznymi im. Pawła Adamowicza w Gdańsku odpowiada za cele i sposoby przetwarzania danych osobowych. Tym samym generalnie w procesach przetwarzania danych realizowanych w swojej działalności Uniwersyteckie Liceum Ogólnokształcące z Oddziałami Dwujęzycznymi im. Pawła Adamowicza w Gdańsku będzie uznawana za administratora danych osobowych.

Na zasadzie wyjątku Szkoła występuje jako procesor przetwarzający dane osobowe w przypadku:
zbierania w imieniu organizatorów formularzy udziału swoich uczniów w konkursie/olimpiadzie organizowanej przez inną jednostkę oświatową, kulturalną lub inny podmiot działający w interesie publicznym;
działania w porozumieniu z Gminą Gdańsk, w związku z uzyskiwaniem dofinansowania ze środków unijnych, krajowych lub wojewódzkich, gdzie Szkoła występuje jako podmiot przetwarzający dane na rzecz Beneficjenta i dalej, na rzecz Instytucji Pośredniczącej.

16) **Powierzanie danych osobowych podwykonawcom**

Zgodnie z artykułem 28 Ogólnego Rozporządzenia o Ochronie Danych Osobowych jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia

odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi rozporządzenia i chroniło prawa osób, których dane dotyczą. Przetwarzanie danych osobowych przez podmiot przetwarzający może odbywać się wyłącznie na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora.
RODO w art. 28 ust. 3 określa szczegółowe wymagania jakie powinna określać odpowiednio sformułowana umowa przetwarzania danych osobowych. Co istotne RODO w swojej treści nie posługuje się pojęciem „Umowy powierzenia", znanym z art. 31 ustawy o ochronie danych osobowych z 1997 roku, jednocześnie nazewnictwo takie zostało przyjęte przez Szkołę Podstawową nr 1 im. Marii Dąbrowskiej we Wrocławiu w związku z obowiązującą na rynku utrwaloną praktyką w tym obszarze.
W toku audytu w Uniwersyteckim Liceum Ogólnokształcące z Oddziałami Dwujęzycznymi w Gdańsku zidentyfikowano, że Szkoła generalnie nie jest podmiotem przetwarzającym dane (sytuacje takie mogą zdarzać się jedynie wpadkowo; np. konkursy organizowane prze inne placówki oświatowe), a generalnie dla swoich procesów jest administratorem danych, który powierza przetwarzanie danych osobowych innym podmiotom.
Zidentyfikowano następujące obszary, w których Szkoła trwale lub często może powierzać przetwarzanie danych osobowych:

- Obsługa IT
- Obsługa w obszarze BHP
- Obsługa prawna
- Utylizacja dokumentów
- Obsługa strony www
- Korzystanie z oprogramowania bazodanowego
- Realizacja wydruków masowych
- Usługi archiwizacji dokumentów
- Usługi fotografa

17) **Udostępnianie danych przez Szkołę innym podmiotom**

Działalność Szkoły nie wiąże się z koniecznością przetwarzania danych osobowych na masową skalę. Szkoła nie udostępnia danych osobowych innym podmiotom w celach komercyjnych. Pozostaje jednak jednostką oświatową i jest zobowiązana do przekazywania określonych raportów oraz informacji do poszczególnych instytucji, zgodnie z powszechnie obowiązującymi przepisami prawa oraz regulacjami prawa miejscowego.

Ponadto udostępnianie danych osobowych ma również miejsce w przypadku podejmowania przez Szkołę współpracy z ośrodkami medycznymi, które angażują się w określone badania zdrowotne uczniów (np. wszawica, choroby skórne, uzębienie). W tych przypadkach administratorem danych osobowych jest podmiot przeprowadzający dane badanie, działający za zgodą Szkoły oraz rodziców lub przedstawicieli prawnych uczniów.

18) **Przetwarzanie przez Szkołę danych wrażliwych**

Przetwarzane przez Uniwersyteckie Liceum Ogólnokształcące z Oddziałami Dwujęzycznymi w Gdańsku dane osobowe generalnie nie mają charakteru wrażliwego. Dane wrażliwe pojawiają się jednak w przypadku, gdy uczniowie mają jakieś schorzenia lub przewlekłe choroby (w tym psychiczne), w przypadkach, gdy rodzice deklarują chęć brania przez ucznia udziału w zajęciach religii, w obszarze przetwarzania danych osobowych pracowników w zakresie ich zdrowotnych zdolności do pracy – w zakresie wymaganym przez przepisy polskiego prawa. Elementy danych wrażliwych pojawiają się również w tym przypadkach, gdzie Szkoła aktywnie działa w zakresie wsparcia psychologiczno-pedagogicznego i w tym zakresie pozyskuje dodatkowe dane o uczniu i/lub jego sytuacji rodzinnej. W przypadkach trudnych uczeń kierowany jest jednak do odrębnej od Szkoły placówki – Poradni Psychologiczno – Pedagogicznej funkcjonującej na terenie Gdańska.

3 KOMPETENCJE I ODPOWIEDZIALNOŚĆ W ZARZĄDZANIU BEZPIECZEŃSTWEM DANYCH OSOBOWYCH

1. Za bezpieczeństwo danych osobowych przetwarzanych w Szkole odpowiada Administrator, który w myśl przepisów RODO, obowiązany jest zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.
2. Do zadań Administratora należy:
   1) wydawanie upoważnień do przetwarzania danych osobowych – wzór upoważnienia określa **załącznik nr 1**;
   2) odwoływanie upoważnień do przetwarzania danych osobowych **–** wzór odwołania upoważnienia określa **załącznik nr 2**;
   3) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych – wzór ewidencji określa **załącznik nr 3,**
   4) ewidencjonowanie oświadczeń osób upoważnionych o zaznajomieniu się z zasadami zachowania bezpieczeństwa danych – wzór oświadczenia określa **załącznik nr 4**,
   5) określanie potrzeb w zakresie stosowanych w Szkole zabezpieczeń, zatwierdzanie rozwiązań i nadzorowanie prawidłowości ich wdrożenia,
   6) podnoszenie świadomości i kwalifikacji osób przetwarzających dane osobowe w Szkole i zapewnienie odpowiedniego poziomu przeszkolenia w tym zakresie,

   Administrator, może wyznaczyć pracownika administracyjnego, który będzie dbał o dokumentację i będzie podlegał dyrektorowi.

   7) prowadzenie nadzoru nad archiwizacją zbiorów danych oraz zabezpieczanie elektronicznych nośników informacji zawierających dane osobowe.
3. Do zadań IDO należy:

1) informowanie Administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
2) monitorowanie przestrzegania przepisów o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony 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 Prezesem Urzędu Ochrony Danych Osobowych,
5) pełnienie funkcji punktu kontaktowego dla Prezesa Urzędu Ochrony Danych Osobowych w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach,
6) pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia.

4. Do zadań ASI należy:
   1) zarządzanie bezpieczeństwem przetwarzania danych osobowych w systemie informatycznym zgodnie z wymogami prawa i wskazówkami Administratora,
   2) doskonalenie metod zabezpieczenia danych przed zagrożeniami związanymi z ich przetwarzaniem,
   3) przydzielanie identyfikatorów użytkownikom systemu informatycznego oraz zaznajamianie ich z procedurami ustalania i zmiany haseł dostępu,
   4) nadzorowanie prac związanych z rozwojem, modyfikacją, serwisowaniem i konserwacją systemu, zapewnienie bezpieczeństwa wewnętrznego i zewnętrznego obiegu informacji w sieci i zabezpieczenie łączy zewnętrznych.
4. Pracownik upoważniony do przetwarzania danych osobowych:
   1) chroni prawo do prywatności osób fizycznych powierzających Szkole swoje dane osobowe poprzez przetwarzanie ich zgodnie z przepisami prawa oraz zasadami określonymi w Polityce;
   2) zapoznaje się zasadami określonymi w Polityce i składa oświadczenie o znajomości tych przepisów;
   3) za przetwarzanie danych osobowych niezgodnie z prawem, celami przetwarzania lub przechowywanie ich w sposób niezapewniający ochrony interesów osób, których te dane dotyczą ponosi odpowiedzialność karną, wynikająca z przepisów ustawy o ochronie danych osobowych lub pracowniczą na zasadach określonych w kodeksie pracy.

4 REALIZACJA PRAW OSÓB, KTÓRYCH DANE SĄ PRZETWARZANE W SZKOLE

1. W Szkole wprowadza się rozwiązania, które pozwalają na realizowanie praw osób, których dane są przetwarzane. W szczególności dotyczy to:
   1) umożliwienia osobom, których dane dotyczą wyrażenia zgody na przetwarzanie danych osobowych (nie dotyczy to danych odnośnie art. 9 ustawy o systemie oświaty; rozporządzenie MENiS z 19 lutego 2002 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji, rozporządzenie MEN z 28 maja 2010 r. w sprawie świadectw, dyplomów państwowych i innych druków szkolnych),
   2) informowania osób, których dane dotyczą o zbieraniu i przetwarzaniu tych danych,
   3) prawa dostępu przysługującego osobom, których dane dotyczą,
   4) prawa osób, których dane dotyczą, do sprostowania danych,
   5) prawa osób, których dane dotyczą, do usunięcia swoich danych („prawa do bycia zapomnianym"),
   6) prawa osób, których dane dotyczą, do ograniczenia przetwarzania danych.
2. Spełnienie obowiązków informacyjnych względem osób, których dane są przetwarzane odbywa się poprzez przekazanie osobom wymaganych prawem informacji przy zbieraniu danych oraz udokumentowanie realizacji tych obowiązków.
3. Warunkiem prawidłowego spełnienia obowiązku informacyjnego wobec osoby, której dane dotyczą, jest przekazanie jej w zwięzłej, przejrzystej i zrozumiałej formie, jasnym i prostym językiem wszelkich informacji, o których mowa w art. 13 i 14 RODO oraz prowadzenie z nią wszelkiej korespondencji, w myśl art. 15-22 i 34 RODO w sprawie przetwarzania danych osobowych.
4. Informacji, o których mowa w pkt. 3 udziela się na piśmie, w tym w stosownych przypadkach – elektronicznie lub w inny sposób (np. ustnie).
5. Informacje podawane na mocy art. 13 i 14 RODO oraz komunikacja i działania podejmowane na mocy art. 15-22 i 34 RODO są wolne od opłat. Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nadmierne, w szczególności ze względu na swój ustawiczny charakter, Szkoła może pobrać opłatę uwzględniającą administracyjne koszty udzielenia informacji.

6. W Szkole określono następujące przypadki zbierania danych osobowych, które wiążą się z obowiązkiem przedstawienia osobom, których dane dotyczą klauzul informacyjnych:

   1. osoby, z którymi Szkoła koresponduje za pośrednictwem poczty elektronicznej

   – w tych przypadkach Szkoła zbiera takie dane jak adresy e-mail, treść korespondencji, dane kontaktowe podawane w stopkach respondentów;

   2. petenci składający różnego rodzaju pisma w placówce – Szkoła zbiera dane osobowe, które są zawarte w takim piśmie; dokładny zakres danych, który może być zawarty w takim piśmie jest trudny z góry do

określenia, dlatego też klauzula informacyjna w tym obszarze musi być odpowiednio szeroka;
3. osoby korzystające ze strony internetowej placówki – zbieranie m.in. ciasteczek, które na gruncie RODO zostały uznane za dane osobowe;
4. przyjmowanie aplikacji rekrutacyjnych do Szkoły – zbieranie danych o uczniach oraz ich rodzicach lub opiekunach prawnych
5. zbieranie danych osobowych kandydatów do pracy oraz w związku z zatrudnieniem (w przypadku pozytywnej rekrutacji);
6. zbieranie danych w związku z wykorzystywaniem w Szkole monitoringu wizyjnego – klauzula wywieszana jest na tablicy na terenie Szkoły ; nadto zastosowano oznaczenia graficzne.

3. Realizacja zadań, o których mowa w pkt. 1 uwzględnia zasady, w tym wyłączenia, które zostały określone w obowiązujących przepisach prawa o ochronie danych osobowych.
4. Dostęp, usunięcie lub ograniczenie przetwarzania danych osobowych musi być zgodne z przepisami prawa, na podstawie których odbywa się przetwarzanie oraz na podstawie przepisów prawa określających zasady przetwarzania dokumentacji archiwalnej.

5. POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

1. Przetwarzanie powierzonych danych może być realizowane wyłącznie przez podmioty, które gwarantują odpowiednie środki techniczne i organizacyjne dające możliwość spełnienia wymogów RODO, w tym w szczególności skutecznie chroniło prawa osób, których dane dotyczą.
2. Przy określaniu minimalnych wymogów, które powinien spełnić podmiot przetwarzający należy brać pod uwagę charakter, skalę i zakres przetwarzania oraz, jeśli to konieczne, uwzględniać wyniki szacowania ryzyka przeprowadzone w Szkole w tym zakresie.
3. Powierzenie przetwarzania danych osobowych odbywa się na podstawie pisemnej umowy lub porozumienia, które wyraźnie określają charakter i cel przetwarzania, przedmiot i czas trwania przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, oraz obowiązki i prawa administratora i podmiotu przetwarzającego.
4. Dokumentacja, na podstawie której następuje powierzenie danych, musi mieć formę pisemną (dopuszcza się prowadzenie tej dokumentacji w formie elektronicznej).
5. Dokumentacja, na podstawie której następuje powierzenie danych, musi gwarantować Administratorowi realizację zadań wynikających z zapisów art. 28 RODO, w tym w szczególności:
   1) możliwość egzekwowania wskazanych w dokumentacji obowiązków podmiotu przetwarzającego,
   2) możliwość przeprowadzanie kontroli/audytów w zakresie realizacji umowy powierzenia,

3) możliwości weryfikacji czy powierzone dane nie zostały przekazane innemu podmiotowi przez przetwarzającego bez zgody („podpowierzenie danych").

6) Zidentyfikowano następujące obszary, w których Szkoła może trwale lub często powierzać przetwarzanie danych osobowych:

1. Obsługa IT
2. Obsługa w obszarze BHP
3. Obsługa prawna
4. Utylizacja dokumentów
5. Obsługa strony www
6. Korzystanie z oprogramowania bazodanowego
7. Realizacja wydruków masowych
7. Usługi archiwizacji dokumentów
9. Usługi fotografa

6. UDOSTĘPNIENIE DANYCH OSOBOWYCH

1. Dostęp do danych osobowych i ich przetwarzanie bez odrębnego upoważnienia Administratora danych osobowych może mieć miejsce wyłącznie w przypadku działań osób i podmiotów uprawnionych na mocy odpowiednich przepisów prawa do dostępu i przetwarzania danych określonej kategorii.
2. Dane osobowe mogą być udostępniane:
   1) podmiotom i organom publicznym działającym w granicach przyznanych im uprawnień, po okazaniu dokumentów potwierdzających te uprawnienia;
   2) stronom postępowań administracyjnych prowadzonych w Szkole, na zasadach określonych w kodeksie postępowania administracyjnego lub odrębnych przepisów **załącznik nr 7**.
3. Administrator odmawia udostępnienia danych osobowych jeżeli spowodowałoby to naruszenie przepisów prawa.

7. ANALIZA RYZYKA

1. W trakcie procesu zarządzania ryzykiem przeprowadzana jest identyfikacja zagrożeń bezpieczeństwa danych osobowych oraz określane są podatności i skutki wystąpienia tych zagrożeń oraz kategoryzacja danych i czynności przetwarzania pod kątem ryzyka, które przedstawiają. **Załącznik nr 9**
2. W ramach procesu zarządzania ryzykiem przeprowadzana jest:
   1) analiza ryzyka dla czynności przetwarzania danych lub ich kategorii;
   2) ocena skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie.
3. Uzyskane, w ramach procesu analizy ryzyka, wyniki są podstawą do dalszego postępowania ze zidentyfikowanymi ryzykami w kontekście wdrożenia

rozwiązań technicznych i organizacyjnych, które pozwolą ochronić dane osobowe przed utratą ich podstawowych atrybutów (poufności, integralności, dostępności, rozliczalności) oraz pozwolą zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania tych danych w Szkole.

4. Ocena skutków czynności przetwarzania dla ochrony danych oraz ich wpływu na naruszenia praw lub wolności osób fizycznych obejmuje analizę i rozpatrywanie możliwych sytuacji i scenariuszy naruszenia ochrony danych osobowych przy uwzględnieniu charakteru, zakresu, kontekstu i celów przetwarzania, oraz różnego prawdopodobieństwa wystąpienia i wagi zagrożenia.
5. W ramach przeprowadzanej oceny, o której mowa w pkt. 4, należy brać pod uwagę wskazane przez Prezesa UODO rodzaje procesów i czynności przetwarzania, dla których wymagane jest przeprowadzenie oceny skutków dla ochrony danych.
6. Analizy w załączniku dokonano dla każdego z procesów zidentyfikowanych w ramach Rejestru Czynności. W przypadku procesów z tej samej kategorii przyjęto analizę zbiorczą, jeżeli takie działanie było uzasadnione zastosowaniem w przetwarzaniu tych samych rozwiązań organizacyjnych, technicznych oraz obejmowało podobny zakres danych osobowych.
7. Elementem dokonanej analizy ryzyka jest Wstępna ocena skutków dla ochrony danych osobowych, której obowiązek przeprowadzenia wynika z art. 35 RODO. Obowiązek przeprowadzenia takiej oceny wynika jednoznacznie z Wytycznych Grupy Roboczej ds. art. 29 z dnia 4 października 2017 roku pt. „Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679". Proces Wstępnej oceny ma na celu określenie, czy dla danego procesu podmiot powinien przeprowadzić pełną Ocenę Skutków dla Ochrony Danych, czyli szeroką i szczegółową analizę, której celem ma być określenie czy podmiot rzeczywiście może realizować dane działanie (czy nie narusza ono praw i wolności osób, których dane dotyczą) oraz jakie wzmożone środki bezpieczeństwa powinien przewidzieć dla takiego działania. Wstępna ocena jest realizowana poprzez zadanie 10 pytań do każdego danego procesu. Jeżeli co najmniej 2 odpowiedzi na pytania są pozytywne to jest to przesłanka za uznaniem konieczności realizacji pełnej Oceny Skutków dla tego procesu. Te pytania to:
8. Czy w procesie realizowana jest ewaluacja lub ocena podmiotu danych, w tym profilowanie i przewidywanie (np. tworzenie profili zachowania lub profili marketingowych)?
9. Czy występuje zautomatyzowane podejmowanie decyzji wywołujące skutki prawne lub podobne istotne skutki wobec podmiotu danych? (np. przetwarzania mogące prowadzić do automatycznej blokady konta, usunięcia danych, odmówienia świadczenia usługi);
10. Czy występuje systematyczne monitorowanie podmiotów danych?
11. Czy przetwarzane są szczególne kategorie danych (np. dane zdrowotne, dane biometryczne)?

12. Czy dane są przetwarzane na dużą skalę? (bierzemy pod uwagę liczbę osób, których dane dotyczą, ilość danych, czas trwania oraz zakres geograficzny przetwarzania);
13. Czy dokonuje się porównania lub połączenia zestawów danych? (np. pochodzących z co najmniej dwóch operacji przetwarzania danych przeprowadzonych w różnych celach lub przez różnych administratorów danych w sposób wykraczający poza uzasadnione oczekiwania osób, których dane dotyczą);
14. Czy przetwarzane są dane osobowe osób wymagających szczególnej opieki (np. dzieci)?
15. Czy występuje innowacyjne wykorzystanie lub zastosowanie rozwiązań technologicznych lub organizacyjnych? (np. połączenie technologii rozpoznającej czytanie maili, monitoring zachowania z analizą chat);
16. Czy występuje transgraniczne przekazywanie danych poza Europejski Obszar Gospodarczy?
17. Czy przetwarzanie samo w sobie „uniemożliwia" osobom, których dane dotyczą, wykorzystanie prawa lub korzystanie z usługi lub umowy? (np. sprawdzanie przez bank klientów w bazie informacji kredytowej, aby podjąd decyzję o zaproponowaniu im pożyczki lub nie).
18.
19. W tym miejscu należy wskazać, że w ramach analizy ryzyka zanotowano jedynie ostateczną odpowiedź, czy dla danego procesu wymagana jest pełna Ocena Skutków dla Ochrony Danych, czy też nie, tj. czy dla danego procesu udzielono co najmniej dwóch pozytywnych odpowiedzi na dziesięć z powyższych pytań.

8. BEZPIECZEŃSTWO W PRZETWARZANIU DANYCH OSOBOWYCH W FORMIE TRADYCYJNEJ

1. Pomieszczenia, w których przetwarzane są dane osobowe, pozostają zawsze pod bezpośrednim nadzorem upoważnionego do ich przetwarzania pracownika. Opuszczenie pomieszczenia musi być poprzedzone przeniesieniem danych osobowych do odpowiednio zabezpieczonego miejsca. Przy planowanej dłuższej nieobecności pracownika pomieszczenie winno być zamknięte na klucz.
2. Klucze do szaf, w których przechowywane są dane osobowe mają jedynie pracownicy upoważnieni do przetwarzania danych osobowych, w zakresie zgodnym z kategorią danych.
3. Korzystanie ze zbiorów danych osobowych przez osoby niezatrudnione w Szkole powinno odbywać się po uzyskaniu upoważnienia lub skonsultowane z Administratorem, w przypadku pracowników upoważnionych do przetwarzania tych danych na podstawie ogólnie obowiązujących przepisów.
4. Upoważnieni pracownicy są zobowiązani do stosowania tzw. „Polityki czystego biurka". Polega ona na zabezpieczaniu (zamykaniu) dokumentów np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy.

5. Upoważnieni pracownicy zobowiązani są do niszczenia dokumentów i wydruków w niszczarkach lub utylizacji ich w specjalnych bezpiecznych pojemnikach z przeznaczeniem do bezpiecznej utylizacji.
6. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. w korytarzach, na kserokopiarkach, drukarkach, w pomieszczeniach ogólnodostępnych.
7. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz, np., na terenach publicznych miejskich lub w lesie.

9. BEZPIECZEŃSTWO W PRZETWARZANIU DANYCH OSOBOWYCH W SYSTEMACH INFORMATYCZNYCH

Zasady bezpiecznego użytkowania systemu informatycznego zawarte są w Instrukcji zarządzania systemem informatycznym, obligatoryjnej do zapoznania się i stosowania przez wszystkich użytkowników systemu informatycznego Szkoły, stanowiącej **załącznik nr 5.**

Zasady korzystania z Internetu:
1. Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych.

2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą osoby upoważnionej do administrowania infrastrukturą IT i tylko w uzasadnionych przypadkach.
3. Użytkownik ponosi odpowiedzialność za szkody w infrastrukturze IT spowodowane przez oprogramowanie instalowane z Internetu.
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo ze względu na zainstalowane na nich szkodliwe oprogramowanie infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem.
5. Zabrania się w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą. W tej sytuacji należy „kliknąć" na ikonę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.
7. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet.

Zasady korzystania z poczty elektronicznej

1. W przypadku przesyłania danych osobowych poza szkołę należy wykorzystywać mechanizmy kryptograficzne (hasłowanie wysyłanych dokumentów lub plików zzipowanych).
2. Każdy użytkownik przed wysłaniem poczty jest zobowiązany sprawdzić poprawność adresu odbiorcy dokumentu.
3. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
4. W celu ochrony przed zainfekowaniem komputera użytkownika i komputerów pracujących w sieci (kryptowirusy) zabrania się otwierania załączników (plików) w mailach nawet od prawdopodobnie znanych użytkownikowi nadawców bez weryfikacji nadawcy.
5. Zabrania się, bez weryfikacji wiarygodności nadawcy „klikać" na hiperlinki w mailach. Nieprzestrzeganie tej zasady może doprowadzić do zainfekowania komputera użytkownika i innych pracujących w sieci.
6. Wszystkie przypadki e-maili budzących podejrzenie należy zgłaszać administratorowi sieci/ informatykowi.
7. Przy wysyłaniu maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW". Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości".
8. Użytkownicy nie mają prawa korzystać z poczty elektronicznej w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub nietycznym i naruszającym cudzą godność i prywatność
9. Użytkownik bez zgody Pracodawcy nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące Pracodawcy, jego pracowników, uczniów, rodziców za pośrednictwem Internetu, w tym przy użyciu elektronicznej skrzynki pocztowej.
10. Wszelkie przesyłane dokumentów, opracowania, jak i innych treści przesyłane przez użytkownika podlegają zasadom ochrony prawa autorskiego i prawa własności przemysłowej, które użytkownik jest obowiązany przestrzegać.

10. NARUSZENIE BEZPIECZEŃSTWA DANYCH OSOBOWYCH

1. Każda osoba upoważniona do przetwarzania danych osobowych w Szkole jest zobowiązana do natychmiastowego powiadamiania Administratora o wystąpieniu incydentu związanego z naruszeniem ochrony danych osobowych.
2. Szczegółowy tryb postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych, został określony w **załączniku nr 6, a załącznik 10** jest rejestrem naruszeń.

11. REJESTR CZYNNOŚCI PRZETWARZANIA

Obowiązek prowadzenia rejestru czynności przetwarzania danych osobowych, wynikający z art. 30 RODO spoczywa na administratorze danych oraz podmiocie przetwarzającym dane. W związku z tym w Szkole zdefiniowano *Rejestr czynności prowadzony przez Administratora* - ***Załącznik 8***.

12. WERYFIKACJA SYSTEMU OCHRONY DANYCH

1. Weryfikacja systemu ochrony danych odbywa się poprzez prowadzenie kontroli okresowych nie rzadziej niż raz w roku.
2. W zależności od potrzeb, część prac w ramach weryfikacji systemu ochrony danych, może zostać zlecone podmiotowi zewnętrznemu.

Niszczenie danych osobowych
1. Usuwanie danych osobowych, polega na:
a) trwałym, fizycznym ich zniszczeniu wraz z ich nośnikami w stopniu uniemożliwiającym ich odtworzenie przez osoby niepowołane przy zastosowaniu powszechnie dostępnych metod,
b) anonimizacji zbiorów danych osobowych polegającej na pozbawieniu danych osobowych, ich zbiorów – cech umożliwiających identyfikację osób fizycznych, których dane dotyczą.
2. Procedura niszczenia danych osobowych:
a) niszczenie danych osobowych następuje wyłącznie na wniosek Administratora i w zgodzie z odrębnymi przepisami,
b) sposób zniszczenia danych osobowych musi być odpowiednio dobrany do rodzaju nośnika danych oraz ich kategorii,
c) niszczenie danych osobowych musi odbywać się komisyjnie, przy czym w komisji musi znajdować się Administrator (lub jego przedstawiciel),
d) zniszczenie danych osobowych musi zostać potwierdzone spisaniem protokołu.
3. Usuwanie danych osobowych jest zależne od rodzaju nośnika, na którym są przechowywane.
a) Dokumentacja tradycyjna (wydruki, notatki, dokumenty itd.) – przy użyciu niszczarki,
b) Nośniki optyczne (płyty CD/DVD) – za pomocą niszczarek.
c) Nośniki elektroniczne (pendrive/karty pamięci/dyski twarde SSD) – korzystając z jednej z dwóch metod: – niszczenie programowe – polegające na wielokrotnym nadpisywaniu danych na nośniku, które uniemożliwiają odczytanie danych, – niszczenie sprzętowe – polegające na trwałym zniszczeniu nośnika za pomocą odpowiednich urządzeń.
d) Nośniki magnetyczne (dyskietki/dyski twarde HDD) – korzystając z jednej z trzech metod: – niszczenie programowe – polegające na wielokrotnym nadpisywaniu danych na nośniku, które uniemożliwiają odczytanie danych, – niszczenie sprzętowe – polegające na trwałym zniszczeniu nośnika za pomocą

odpowiednich urządzeń, oprócz sposobów niszczenia danych dostępnych dla nośników elektronicznych, – demagnetyzacji nośników.

13 WYKAZ POMIESZCZEŃ, TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

1. Przetwarzaniem danych osobowych jest wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza tych, które wykonuje się w systemie informatycznym.
2. Dane osobowe przetwarzane są na terenie Szkoły
3. Budynek, w którym usytuowana jest szkoła jest zabezpieczany codziennie i całodobowo przez strażnika, system elektronicznego zabezpieczenia (SSWiN) oraz system ppoż. przekazuje sygnały alarmowe całodobowo do portierni Biblioteki Głównej UG, jest monitoring systemu CCTV. Ponadto codziennie w godzinach od 6.00 do 22.00 zabezpieczana jest portiernia górna przez strażnika SU.
4. Ze względu na nagromadzenie danych osobowych szczególnie chronione powinny być pomieszczenia, zgodnie z poniższym wykazem.

Budynek	Rodzaj dokumentów	Miejsce przechowywania
	Dziennik elektroniczny	Dostęp z komputerów w każdej klasie. Każdy nauczyciel ma swoje konto zabezpieczone hasłem zmienianym raz w miesiącu. Baza danych zabezpiecza firma „Vulcan" Laptop zabezpieczony hasłem,
	Dzienniki zajęć specjalistycznych	Pokój nauczycielski dostęp mają tylko nauczyciele (każdy ma swój klucz do zamykanej szafki). Pedagog i Psycholog własne pokoje zamykane na klucz.
	Zeszyty/dzienniki wychowawcy	Pokój nauczycielski dostęp mają tylko nauczyciele (każdy ma swój klucz).
	Dzienniki zajęć pozalekcyjnych	Pokój nauczycielski dostęp mają tylko nauczyciele (każdy ma swój klucz).
	Dziennik pedagoga	Pokój pedagoga – zamykany na klucz
	Księga ewidencji uczniów	Sekretariat szkoły – wersja papierowa oraz w formie elektronicznej
	Księga uczniów	Sekretariat szkoły oraz w formie elektronicznej
	Dane dot zdrowia	Gabinet pielęgniarki szkolnej
	Arkusze ocen	Sekretariat szkoły - drukowane oraz w formie elektronicznej

	Dokumenty z nadzoru pedagogicznego	Gabinet dyrektora szkoły – klucz portiernia i Dyrektor
	Dokumentacja pomocy pp	Sekretariat –oraz pokój pedagoga
	Ewidencja uczniów przystępujących do sprawdzianu/egzaminu zewnętrznego	Sekretariat szkoły
	Dokumentacja opiekuńczo-wychowawcza	Gabinet dyrektora szkoły – gabinet pedagoga szkolnego
	Arkusz organizacyjny szkoły	Sekretariat szkoły
	Postępowanie administracyjne w sprawie realizacji obowiązku nauki	Sekretariat szkoły
	Decyzje o odroczenie obowiązku szkolnego	Sekretariat szkoły
	Podania ubiegających się o pracę	Sekretariat szkoły
	Ewidencja wydanych świadectw, zaświadczeń i legitymacji	Sekretariat szkoły
	Księga kontroli zewnętrznej	Sekretariat szkoły
	Lista obecności	Sekretariat szkoły
	Dziennik korespondencyjny	Sekretariat szkoły
	Rejestr upoważnień	Sekretariat szkoły
	protokóły wypadkowe	Sekretariat szkoły
	Lokalne bazy SIO – uczniowie i budynki	Sekretariat szkoły
	Teczki awansu zawodowego	Sekretariat szkoły
	Akta osobowe	Sekretariat szkoły
	Listy płac	Pokój głównej księgowej i referenta – Puck, siedziba Fundacji
	Dokumentacja Komisji Zdrowotnej	Sekretariat szkoły
	Dokumentacja kadrowa	Pokój głównej księgowej i referenta – Puck, siedziba Fundacji
	Lokalne bazy SIO - sprawy kadrowe	Sekretariat szkoły

Opis pomieszczeń tworzących obszar, w którym są przetwarzane dane osobowe

1. Uniwersyteckie Liceum Ogólnokształcące z Oddziałami Dwujęzycznymi mieści się przy ul. Traugutta 92 w Gdańsku, są tu oprócz sal lekcyjnych: sekretariat, dwa pokoje Wicedyrektorów, pokój Dyrektora, gabinet pedagoga szkolnego, gabinet pielęgniarki szkolnej.
2. Sekretariat oraz pokoje Wicedyrektora i Dyrektora znajdują się na piętrze budynku, w pokojach tych przetwarzane są dane osobowe ręcznie oraz poprzez system informatyczny. Dokumentację papierową oraz komputerowe nośniki informacji (dyski) przechowuje się w szafach zamykanych na klucze, które są w posiadaniu Dyrektora i sekretarki szkolnej. Komputery zasilane są baterią umożliwiają prawidłowe zamknięcie systemu komputerowego w razie spadku lub braku prądu. W komputerze znajduje się program SIO – system informacji oświatowej. Program może uruchomić tylko pracownik upoważniony do jego otwarcia przy użyciu odpowiednich haseł.
3. Pokój nauczycielski znajduje się na piętrze budynku. W pokoju tym przetwarzane są dane osobowe uczniów i ich rodziców ręcznie i przez system informatyczny poprzez dostęp do komputera z edziennikiem. Dokumentację papierową przechowuje się podczas zajęć dydaktycznych w szafie zamykanej na klucz w pokoju nauczycielskim.
4. Pokój pedagoga szkolnego znajduje się na 3 poziomie i przystosowany jest do pracy dla jednej osoby. W pokoju tym przetwarzane są dane osobowe ręcznie oraz poprzez system informatyczny. Dokumentację papierową oraz komputerowe nośniki informacji tj. dyski przechowuje się w szafach zamykanych na klucze, które są w posiadaniu pedagoga. Komputer może uruchomić tylko pracownik upoważniony do jego otwarcia przy użyciu odpowiednich haseł.
5. Pieczęcie z nazwą i siedzibą instytucji oraz imienne są przechowywane w szafie pancernej Uniwersyteckiego Liceum Ogólnokształcącego z Oddziałami Dwujęzycznymi.
6. Przesyłki zawierające dane osobowe przesyła się jako polecone z ewentualnym zwrotnym potwierdzeniem odbioru oraz zabezpieczone w sposób uniemożliwiający zapoznanie się z ich treścią przez osoby nieupoważnione .
7. Dokumenty zawierające dane osobowe przekazuje się do archiwum/kas pancernych mieszczących się w budynku Szkoły na 2 poziomie w sekretariacie szkoły, po okresie przydatności dokumenty zawierające dane osobowe niszczy się na podstawie decyzji Dyrektora komisyjnie, w warunkach gwarantujących zabezpieczenie danych osobowych w sposób gwarantujący uniemożliwienie ich odtworzenia, wykazy i spisy zdawczo - odbiorcze dokumentów zawierające dane osobowe przekazywanych do archiwum oraz protokoły zniszczenia dokumentów przechowuje administrator danych. Dostęp do archiwum szkolnego posiada sekretarka szkolna oraz dyrektor szkoły.
8. Dokumenty zawierające dane osobowe niezbędne do pracy w terenie należy przechowywać w warunkach gwarantujących ich należytą ochronę.

9. Dane osobowe pracowników Uniwersyteckiego Liceum Ogólnokształcącego z Oddziałami Dwujęzycznymi są przetwarzane w budynku Szkoły oraz siedzibie Fundacji Pozytywne Inicjatywy w Pucku.

14 WYKAZ PROGRAMÓW i PLATFORM ONLINE STOSOWANYCH W SZKOLE:

- Windows
- Linux,
- Office,
- Libre office
- Dziennik elektroniczny VULCAN
- SIO- System Informacji Oświatowej,
- Program KADROWO-PŁACOWY,
- Płatnik- program obsługujący przelewy danych do ZUS,
- RPS.ms
- ODPN
- CROD

15 RADA RODZICÓW

Rada Rodziców w obszarze swojej podstawowej działalności co do zasady nie spełnia kryteriów do uznania za odrębnego od Uniwersyteckiego Liceum Ogólnokształcącego z Oddziałami Dwujęzycznymi - administratora danych (kryterium samodzielnego decydowania o celach i środkach przetwarzania danych osobowych co do zasady nie zostaje spełnione). Z tej perspektywy do wzorów upoważnień do przetwarzania danych osobowych dodano również upoważnienia do przetwarzania danych przez członków Rady Rodziców.
Jednocześnie należy wskazać, że Szkoła w określonych przypadkach będzie uznawać Radę Rodziców (jej członków działających w otoczeniu Szkoły) za odrębnego administratora danych, który jest obowiązany do samodzielnego zadbania o prawidłowość przetwarzania danych osobowych. Dotyczyć to będzie w szczególności:

1. przypadków, gdy sposób funkcjonowania Rady Rodziców w sposób istotny oddzieli się od Szkoły – w szczególności prace Rady Rodziców będą odbywały się poza placówką, poza placówką będzie przechowywana dokumentacja zawierająca dane osobowe, Rada Rodziców będzie odmawiać prawa do nadzoru Rady ze strony Inspektora Ochrony Danych Osobowych lub będzie odmawiać zastosowania się do jego wskazań;

2. dla procesów przetwarzania, w których Rada Rodziców będzie działała całkowicie z własnej inicjatywy poza auspicjami Szkoły – np. prowadzenie samodzielnego profilu w mediach społecznościowych (np. fanpage Rady Rodziców na Facebook'u) lub inne przypadki samodzielnego publikowania danych osobowych (uczniów, nauczycieli).

16 KONKURSY

Uczniowie Uniwersyteckiego Liceum Ogólnokształcącego z Oddziałami Dwujęzycznymi mogą brać udział w wielu konkursach w trakcie roku szkolnego. Część konkursów ma charakter wewnętrzny (tylko dla uczniów Szkoły), a część konkursów ma charakter międzyszkolny (regionalny, ponadregionalny, ogólnopolski). Dla przypadków konkursów wewnętrznych Szkoła nie musi realizować żadnych dodatkowych czynności w obszarze przetwarzania danych osobowych. W tym zakresie, zgodnie z Testem klauzuli interesu publicznego (Rozdział IV Polityki Ochrony Danych Osobowych) Szkoła działa w granicach swojej misji edukacyjnej, a podejmowane czynności przetwarzania danych osobowych nie wykraczają poza bieżące funkcjonowanie placówki.

W przypadku pozostałych konkursów sytuacja przedstawia się już nieco inaczej. Tam gdzie Szkoła jako organizator konkursu zbiera dane osobowe uczniów innych placówek w celu realizacji konkursu, powinna uzyskać odrębną zgodę rodziców/przedstawicieli ustawowych uczniów na ich udział w konkursie. Taka zgoda w świetle art. 6 ust.1 lit. a RODO będzie oznaczała również zgodę na przetwarzanie danych osobowych tych uczniów w celu realizacji konkursu. Przy okazji zbierania takiej zgody Szkoła zobowiązana jest wypełnić obowiązek informacyjny w rozumieniu art. 13 RODO. Jeżeli dodatkowo Szkoła planuje publikować zdjęcia z przebiegu konkursu w Internecie, w mediach społecznościowych, zobowiązana jest uzyskać na to odrębną zgodę.

Jak wskazano powyżej, Szkoła - organizator ma obowiązek uzyskiwać zgody rodziców / przedstawicieli ustawowych na udział dziecka w konkursie. Powinna również wypełnić obowiązek informacyjny.

Każda Szkoła – uczestnik przystępując do udziału w Konkursie organizowanego przez Szkołę równocześnie akceptuje obok regulaminu samego konkursu również reguły przetwarzania danych osobowych z nim związanych. W ten sposób spełnione są warunki powierzenia przetwarzania danych określone przez art. 28 RODO.

17 POSTANOWIENIA KOŃCOWE

1. Osoby przetwarzające dane osobowe zobowiązane są do stosowania postanowień zawartych w niniejszym dokumencie oraz pozostałej dokumentacji, która uszczegóławia wymagania i zasady ochrony danych osobowych.

2. Przypadki, nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako naruszenie obowiązków służbowych.
3. Polityka oraz pozostała dokumentacja, która uszczegóławia wymagania i zasady ochrony danych osobowych może być udostępniania osobom trzecim, jeżeli nie zawiera w swojej treści i w załącznikach szczegółowych informacji o wdrożonych w Szkole zabezpieczeniach danych osobowych oraz innych informacji prawnie chronionych.

Wykaz załączników

Załącznik nr 1 – Upoważnienie szkoły do przetwarzania danych osobowych uczniów i rodziców
Załącznik nr 2 – Odwołanie upoważnienia
Załącznik nr 3 – Ewidencja osób upoważnionych do przetwarzania danych osobowych
Załącznik nr 4 – Oświadczenie pracownika o zapoznaniu się z zasadami zachowania bezpieczeństwa danych osobowych
Załącznik nr 5 – Instrukcja zarządzania systemem informatycznym
Załącznik nr 6 – Zasady postępowania w przypadku wykrycia naruszenia ochrony danych osobowych.
Załącznik nr 7 – Wniosek o udostępnienie danych osobowych
Załącznik nr 8 - Rejestr czynności Administratora
Załącznik nr 9 – Analiza ryzyka
Załącznik nr 10 – Rejestr naruszeń