SZKOŁA PODSTAWOWA
w NAKLI
77-127 Nakla, ul. Szkolna 6

ZARZĄDZENIE NR 4/2018/2019

Dyrektora Szkoły Podstawowej w Nakli

z dnia 1 lutego 2019 r.

w sprawie wprowadzenia Polityki ochrony danych osobowych w Szkole Podstawowej w Nakli

Na podstawie art. 24 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE)2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. U. UE L. 206. 119. 1) zarządza się, co następuje:

§ 1.

Wprowadza się Politykę ochrony danych osobowych w Szkole Podstawowej w Nakli stanowiącą załącznik do niniejszego zarządzenia

§ 2.

Polityka ochrony danych osobowych ma zastosowanie w Szkole Podstawowej w Nakli do wszystkich stanowisk pracy, gdzie przetwarzane są dane osobowe.

§3.

Z treścią Polityki ochrony danych osobowych zobowiązani są zapoznać się wszyscy pracownicy Szkoły Podstawowej w Nakli przetwarzający dane osobowe.

§ 4.

Zobowiązuje się wszystkich pracowników Szkoły Podstawowej w Nakli do przestrzegania zasad wynikających z Polityki ochrony danych osobowych.

§ 5

Traci moc zarządzenie 22/2017/2018 z 25 maja 2018 r. w sprawie wprowadzenia Polityki ochrony danych osobowych w Szkole Podstawowej w Nakli.

§ 6

Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR SZKOŁY
mgr inż. Jan Pyrcka

POLITYKA OCHRONY DANYCH OSOBOWYCH

Szkoły Podstawowej w Nakli
ul. Szkolna 6. 77-127 Nakla

Data wprowadzenia:	
Wersja:	**1**
Daty utworzenia:	**01.02.2019r**
Opracował:	**Piotr Przyborowski (IOD)**
Zatwierdził:	

SPIS TREŚCI:

1. Wykaz podstawowych definicji i skrótów

Ilekroć w niniejszej Polityce Bezpieczeństwa Danych Osobowych mowa o:

Administratorze Danych Osobowych (ADO) – Szkoła Podstawowa w Nakli;

Administratorze Systemu Informatycznego (ASI) – rozumie się przez to pracownika Administratora Danych Osobowych lub inne osoby odpowiedzialne za funkcjonowanie systemów i sieci teleinformatycznych oraz za przestrzeganie zasad i wymogów bezpieczeństwa systemów i sieci teleinformatycznych;

Inspektorze Ochrony Danych (IOD) – rozumie się przez to osobę odpowiedzialną za bieżący nadzór stosowania przepisów dot. ochrony danych osobowych;

Osobie upoważnionej – rozumie się przez to osobę upoważnioną przez Administratora Danych Osobowych do przetwarzania danych osobowych. Osobą upoważnioną może być

pracownik Spółki, osoba wykonująca prace na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, a także osoba odbywająca wolontariat, praktykę lub staż;

Danych osobowych – rozumie się przez to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą");

Możliwej do zidentyfikowania osobie fizycznej – rozumie się przez to 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;

Przetwarzaniu danych osobowych – rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

Zbiorze danych osobowych – rozumie się przez to uporządkowany zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

Podmiocie przetwarzającym – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora Danych Osobowych;

Odbiorcy danych – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postepowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;

Systemie informatycznym (SI) – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;

Bezpieczeństwie danych osobowych – rozumie się przez to zespół zasad, jakimi należy się kierować projektując oraz wykorzystując systemy i aplikacje służące do przetwarzania danych osobowych, by w każdych okolicznościach dostęp do nich był zgodny z założeniami i zapewniał ich poufność, integralność oraz dostępność;

Poufności danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom lub podmiotom;

Integralności danych – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

Dostępności danych – rozumie się przez to właściwość zapewniającą, że dane są osiągalne i możliwe do wykorzystania na żądanie, w założonym czasie, przez uprawnioną osobę lub podmiot;

Zgodzie osoby, której dane dotyczą – rozumie się przez to dobrowolne, konkretne, świadome i jednoznaczne okazanie woli przez osobę, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwalające na przetwarzanie dotyczących jej danych osobowych;

Państwie trzecim – rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego;

Incydencie – rozumie się przez to naruszenie bezpieczeństwa danych osobowych;

Zagrożeniu – rozumie się przez to potencjalną możliwość wystąpienia incydentu;

Naruszeniu ochrony danych osobowych – rozumie się przez to naruszenie bezpieczeństwa danych osobowych prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

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).

2. Wprowadzenie

1) Polityka Ochrony Danych Osobowych (Polityka, PODO) określa reguły przetwarzania danych osobowych oraz sposobów ich zabezpieczenia, jako zestaw praw, zasad i zaleceń regulujących sposób ich zarządzania, ochrony i dystrybucji w SP w Nakli.
2) Polityka zawiera informacje dotyczące rozpoznawania procesów przetwarzania danych osobowych oraz wprowadzonych zabezpieczeń techniczno-organizacyjnych, zapewniających ochronę przetwarzanych danych osobowych.
3) Niniejszy dokument jest zgodny z obowiązującymi przepisami prawa, a w szczególności z Rozporządzeniem 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

3. Cele Polityki Ochrony Danych Osobowych

Celem Polityki Ochrony Danych Osobowych jest określenie oraz wdrożenie zasad bezpieczeństwa i ochrony danych osobowych przetwarzanych w SP w Nakli, a w szczególności:

1) zapewnienie spełnienia wymagań prawnych;

2) zapewnienie poufności, integralności oraz rozliczalności danych osobowych przetwarzanych w firmie;
3) podnoszenie świadomości osób przetwarzających dane osobowe;
4) zaangażowanie osób przetwarzających dane osobowe firmy w ich ochronę.

4. Zakres stosowania

1) Politykę Ochrony Danych Osobowych stosują wszystkie podmioty przetwarzające dane osobowe w imieniu Administratora Danych Osobowych.

2) Politykę stosuje się do wszelkich czynności, stanowiących w myśl RODO, przetwarzanie danych osobowych. Bez względu na źródło pochodzenia danych osobowych, ich zakres, cel zebrania, sposób przetwarzania lub czas przetwarzania, stosowane są zasady ujęte w Polityce.

5. Struktura organizacji ochrony danych osobowych

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 Osobowych,
2) Inspektor Ochrony Danych,
3) Administrator Systemów Informatycznych,
4) Osoby upoważnione do przetwarzania danych osobowych.

5.1. Administrator Danych Osobowych

1) Administrator Danych Osobowych odpowiada za zakres i bezpieczeństwo przetwarzania danych osobowych w SP w Nakli.

2) Administrator jest odpowiedzialny za przestrzeganie przepisów RODO i musi być w stanie wykazać ich przestrzeganie (tzw. zasada rozliczalności RODO). Aby to zrealizować, Administrator prowadzi działania zapisane w punkcie 6 niniejszej Polityki.

3) Administrator zapewnia i stosuje odpowiednie środki informatyczne, techniczne i organizacyjne, zapewniając ochronę przetwarzanych danych osobowych odpowiednią do wyników analizy ryzyka.

5.2. Inspektor Ochrony Danych

1) Do zadań Inspektora Ochrony Danych należy:

a) monitorowanie przestrzegania RODO, innych przepisów Unii oraz prawa polskiego o ochronie danych oraz polityk administratora w dziedzinie ochrony danych osobowych,
b) przygotowanie lub weryfikacja i aktualizacja umów, regulaminów, polityki ochrony danych osobowych, zapytań, klauzul informacyjnych i zgód oraz innych dokumentów związanych z ochroną danych osobowych,
c) przeprowadzenie oceny skutków przetwarzania danych osobowych dla ich ochrony oraz monitorowanie jej wykonania,
d) prowadzenie rejestru czynności przetwarzania danych osobowych,
e) analiza stosowanych techniczno-organizacyjnych środków ochrony, bezpieczeństwa fizycznego oraz informatycznego związanych z przetwarzaniem danych osobowych,
f) organizowanie i prowadzenie szkoleń dla pracowników z zakresu ochrony danych osobowych,
g) zarządzanie upoważnieniami oraz ewidencją osób upoważnionych do przetwarzania danych osobowych,
h) przeprowadzenie okresowego audytu zgodności oraz przygotowanie raportu,
i) prowadzenia audytów podmiotów, którym Zleceniodawca powierzył przetwarzanie danych osobowych,
j) pełnienie funkcji punktu kontaktowego dla organu nadzorczego ds. ochrony danych osobowych,
k) uczestnictwo podczas kontroli organu nadzorczego,
l) pełnienie funkcji punktu kontaktowego dla osób, których dane dotyczą,
m) wsparcie przy rozpatrywaniu zapytań i skarg osób, których dane dotyczą,
n) nadzór nad procesem obsługi naruszeń ochrony danych osobowych.

2) W ramach wykonywania swoich obowiązków IOD przeprowadza okresowe szkolenia z zakresu ochrony danych osobowych, co dokumentowane jest w Wykazie przeprowadzonych szkoleń (Załącznik PODO 7)

5.3. Administrator Systemów Informatycznych

Do zadań ASI należy:

1) prowadzenie rejestru nadanych uprawnień do systemów informatycznych,
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 naruszeń w systemie zabezpieczeń,
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.

5.4. Osoby upoważnione do przetwarzania danych osobowych

1) Do obowiązków osób upoważnionych do przetwarzania danych osobowych należy:

a) zapoznanie się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami Polityki Ochrony Danych Osobowych i Instrukcji Zarządzania Systemami Informatycznymi (Załącznik PODO 5);

b) stosowanie się do zaleceń Inspektora Ochrony Danych;

c) przetwarzania danych osobowych wyłącznie w zakresie ustalonym indywidualnie przez Administratora Danych Osobowych w pisemnym upoważnieniu i tylko w celu wykonywania nałożonych obowiązków służbowych;

d) niezwłoczne informowanie Inspektora Ochrony Danych o wszelkich nieprawidłowościach dotyczących bezpieczeństwa danych osobowych przetwarzanych w firmie;

e) ochronę danych osobowych oraz środków wykorzystywanych do przetwarzania danych osobowych przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem;

f) bezterminowe zachowanie w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia;

2) Każda osoba, która uzyskała upoważnienie do przetwarzania danych, zobowiązana jest do ich ochrony w sposób zgodny z przepisami RODO, oraz postanowieniami Polityki.

3) Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia.

6. Podstawowe zasady ochrony danych osobowych

1) Przetwarzanie danych osobowych w strukturze Administratora Danych odbywa się zgodnie z ogólnymi zasadami przetwarzania danych osobowych określonymi w art. 5 RODO. Oznacza to, że dane osobowe przetwarza się:

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

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

c) w sposób przejrzysty dla osób, których dane dotyczą (*zasada przejrzystości*),

d) w konkretnych, wyraźnych i prawnie uzasadnionych celach (*zasada ograniczenia celu*),

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

f) przy uwzględnieniu ich prawidłowości i ewentualnego uaktualniania (*zasada prawidłowości*),

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

h) w sposób zapewniający odpowiednie bezpieczeństwo (*integralność i poufność*).

2) SP w Nakli prowadzi Rejestr czynności przetwarzania danych osobowych (Załącznik PODO 15), który stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.

7. Upoważnienie do przetwarzania danych osobowych

1) Do przetwarzania danych osobowych i obsługi zbiorów informatycznych zawierających te dane mogą być dopuszczone wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych (wzór - Załącznik PODO 8) wydane przez Administratora Danych Osobowych.
2) Administrator Danych Osobowych prowadzi rejestr osób upoważnionych do przetwarzania danych osobowych (wzór - Załącznik PODO 11).

8. Powierzenie przetwarzania danych osobowych

1) Administrator Danych Osobowych może zlecić innemu podmiotowi przetwarzanie danych osobowych w celu realizacji określonego zadania (wzór umowy - Załącznik PODO 10)
2) W sytuacji powierzenia przetwarzania danych osobowych podmiotowi zewnętrznemu, w umowie powierzenia przetwarzania danych osobowych określa się przede wszystkim przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.

9. Udostępnianie danych osobowych

1) Dane osobowe udostępnia się na wniosek o udostępnienie danych (wzór - Załącznik PODO 9).

2) Wniosek o udostepnienie danych, który wpłynął do SP w Nakli rozpatruje Właściciel zbioru.
3) Wniosek o udostepnienie danych osobowych, którego sposób rozpatrzenia budzi uzasadnione wątpliwości, może zostać przesłany, wraz z informacjami niezbędnymi dla jego rozpatrzenia, do Inspektora Ochrony Danych w celu zajęcia stanowiska w sprawie. Do wniosku dołącza się projekt odpowiedzi wraz z uzasadnieniem.
4) Informacje, zawierające dane osobowe są udostępniane uprawnionym podmiotom:
   a) w formie wydruku listem poleconym lub za potwierdzeniem osobistego odbioru,
   b) w drodze teletransmisji danych (w sposób gwarantujący poufność przesyłanych danych),
   c) na elektronicznych nośnikach informacji, za potwierdzeniem odbioru,
   d) w inny sposób określony przepisami prawa lub umową.
5) Udostępniane dane osobowe podlegają kontroli przez Właściciela zbioru, z którego one pochodzą.
6) Rejestr przypadków udostepnienia danych prowadzony jest przez Właścicieli zbiorów w wersji elektronicznej lub papierowej (wzór - Załącznik PODO 12).
7) Właściciel zbioru zobowiązany jest umożliwić dostęp Inspektorowi Ochrony Danych do prowadzonych ewidencji udostępnień.

10. 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 w tym, w szczególności:
   a) prawo do wycofania wyrażonej zgody (art. 7 ust. 3 RODO),
   b) prawo dostępu przysługujące osobie, której dane dotyczą (art. 15 RODO),
   c) prawo do sprostowania danych (art. 16 RODO),
   d) prawo do usunięcia danych (*prawo do bycia zapomnianym*) (art. 17 RODO),
   e) prawo do ograniczenia przetwarzania (art. 18 RODO),
   f) prawo do przenoszenia danych (art. 20 RODO),
   g) prawo sprzeciwu (art. 21 RODO),
   h) prawo do niepodlegania decyzjom opartym na zautomatyzowanym przetwarzaniu (art. 22 RODO).
2. Procedura realizacji praw osób, których dane dotyczą stanowi Załącznik PODO 1 do Polityki.

11. Ochrona danych osobowych w fazie projektowania oraz domyślna ochrona osób, których dane dotyczą

Administrator Danych Osobowych uwzględni ochronę danych i prywatność na

każdym etapie tworzenia oraz istnienia technologii obejmującej ich przetwarzanie. W tym celu stosuje zasady:

1) privacy by design, której celem jest „wbudowanie" zasad ochrony prywatności w każdy projekt zakładający przetwarzanie danych osobowych w taki sposób, aby od samego początku jego istnienia ochrona prywatności stanowiła jego część składową

2) privacy by default, która zakłada ochronę prywatności, jako domyślne ustawienie każdego programu (systemu), a zmiana takiego ustawienia powinna następować jedynie na wyraźne żądanie użytkownika programu.

12. Analiza ryzyka i ocena skutków dla ochrony danych

1) Analiza ryzyka przetwarzania danych osobowych w SP w Nakli wykonywana jest przy użyciu programu komputerowego ARDO SMALL 2.0, firmy F-tec. F-tec jest firmą doradczą, specjalizującą się w świadczeniu usług z zakresu bezpieczeństwa informacji, oraz producentem specjalistycznego oprogramowania z zakresu bezpieczeństwa informacji niejawnych oraz danych osobowych.
2) Ocenę skutków dokonuje się jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Przeprowadzona jest ona zgodnie z Procedurą będącą Załącznikiem PODO 2 do niniejszej Polityki.

13. Obszary przetwarzania danych osobowych

1) W SP w Nakli dane osobowe przetwarzane są w ramach zbiorów danych osobowych, a obszary możliwego przetwarzania danych osobowych określa Załącznik PODO 14 do niniejszej Polityki.
2) Osoby upoważnione do przetwarzania danych osobowych mogą przetwarzać dane tylko wyznaczonych do tego miejscach z zachowaniem dedykowanego do tej czynności - sprzętu oraz wszelkich innych urządzeń.
3) Wynoszenie zbiorów danych osobowych poza obszar przetwarzania możliwy jest za wyłączną zgodą Administratora Danych.

14. Charakterystyka zbiorów danych osobowych

Inspektor Ochrony Danych odpowiedzialny jest za prowadzenie i przechowywanie dokumentacji zawierającej wykaz wszystkich zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych. Aktualny wykaz zbiorów danych osobowych zawarto w Załączniku PODO 13.

15. Przeglądy, aktualizacje i retencja danych osobowych

1) Polityka podlega okresowemu przeglądowi pod kątem jej adekwatności, nie rzadziej niż raz do roku.
2) Przeglądu Polityki dokonuje Administrator Danych Osobowych we współpracy z Inspektorem Ochrony Danych
3) Przegląd powinien obejmować, w szczególności ocenę adekwatności Polityki do:
   a) procesów funkcjonujących w strukturach Administratora Danych,
   b) obowiązujących przepisów prawa odnoszących się do ochrony danych osobowych, którym podlega Administrator Danych.
4) W każdym przypadku, gdy zmianie ulegają przepisy prawa będące źródłem wskazanych w Polityce obowiązków lub zaistnieją istotne zmiany faktyczne w ramach struktury Administratora Danych przegląd Polityki wykonywany jest niezwłocznie.
5) Jeżeli w wyniku przeglądu Polityki stwierdzona zostanie konieczność aktualizacji jej zapisów, ADO dokonuje aktualizacji Polityki w wymaganym zakresie.
6) Ustalanie zasad i terminów retencji danych osobowych określa Procedura będąca Załącznikiem PODO 4 do niniejszej Polityki.

16. Zarządzanie naruszeniami bezpieczeństwa danych osobowych

Procedura postępowania z naruszeniami ochrony danych osobowych stanowi Załącznik PODO 3 do Polityki.

17. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

Inspektor Ochrony Danych odpowiedzialny jest za prowadzenie i przechowywanie dokumentacji zawierającej określone środki techniczne i organizacyjne niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych. Aktualny opis stosowanych środków technicznych i organizacyjnych zawarto w Załączniku PODO 6

18. Przekazywanie danych osobowych poza Polskę

1) Administrator Danych Osobowych może przekazywać dane osobowe do:
   a) państw Europejskiego Obszaru Gospodarczego;

b) pozostałych państw (państwa trzecie).

2) Przekazywanie danych osobowych w ramach EOG traktuje się tak, jakby były przetwarzane na terenie Polski.

3) W przypadku przekazywania danych osobowych do państwa trzeciego, przekazywanie następuje zgodnie z Rozdziałem V art. 44 – 49 RODO.

19. Postanowienia końcowe

W sprawach nieuregulowanych w niniejszej Polityce Bezpieczeństwa Danych Osobowych mają zastosowanie przepisy Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. 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).

20. Załączniki

1) Załącznik PODO 1 – Procedura Realizacja praw osób, których dane dotyczą,
2) Załącznik PODO 2 – Procedura Analiza ryzyka i ocena skutków dla ochrony danych,
3) Załącznik PODO 3 – Procedura Naruszenie ochrony danych osobowych,
4) Załącznik PODO 4 – Procedura Retencja danych osobowych,
5) Załącznik PODO 5 – Instrukcja Zarządzania Systemami Informatycznymi,
6) Załącznik PODO 6 – Opis stosowanych środków technicznych i organizacyjnych ochrony danych osobowych,
7) Załącznik PODO 7 – Wzór Wykazu szkoleń z zakresu ochrony danych osobowych,
8) Załącznik PODO 8 – Wzór Upoważnienia do przetwarzania danych osobowych,
9) Załącznik PODO 9 – Wzór Wniosku o udostępnienie danych ze zbioru danych osobowych,
10) Załącznik PODO 10 – Wzór Umowy powierzenia przetwarzania danych osobowych,
11) Załącznik PODO 11 – Wzór Rejestru osób upoważnionych do przetwarzania danych osobowych,
12) Załącznik PODO 12 – Wzór Rejestru udostępnień danych osobowych,
13) Załącznik PODO 13 – Wzór Wykazu zbiorów danych osobowych,

14) Załącznik PODO 14 – Wzór Obszarów przetwarzania danych osobowych,

15) Załącznik PODO 15 – Wzór Rejestru czynności przetwarzania danych osobowych.

Załącznik PODO 7

WYKAZ SZKOLEŃ Z ZAKRESU OCHRONY DANYCH OSOBOWYCH

Lp.	Data szkolenia	Przedmiot szkolenia	Prowadzący	Imię i nazwisko	Podpis

Załącznik PODO 8

UPOWAŻNIENIE Nr *...../2019*

- **do przetwarzania danych osobowych**

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 119) – dalej zwanego RODO

z dniem **……..** upoważniam Panią/Pana: **……**
zatrudnioną/-nego na stanowisku: **……...**
do przetwarzania danych osobowych w związku z wykonywaniem czynności wynikających z obowiązków służbowych na stanowisku pracy i poleceń przełożonego.

Niniejsze upoważnienie jest ważne w okresie od **……** do **……**.
W przypadku brak terminu ważności upoważnienia, upoważnienie obowiązuje do zakończenia stosunku pracy z osobą upoważnioną.

Zobowiązuję Panią/Pana do zachowania w tajemnicy danych osobowych oraz znanych Pani/Panu sposobów zabezpieczenia danych osobowych stosowanych w …… (dalej Administrator Danych), przez cały okres zatrudnienia u Administratora Danych / świadczenia usług na rzecz Administratora Danych, jak również po ustaniu zatrudnienia / świadczenia usług.

……..……., dn. ……..
..... (miejscowość) (data)
(pieczęć i podpis Administratora Danych)

- _____

- ***Oświadczenie osoby upoważnionej***

Oświadczam, że zapoznałem się i rozumiem zasady dotyczące ochrony danych osobowych stosowane przez Administratora Danych oraz zobowiązuję się do ich przestrzegania, a w szczególności do zachowania w tajemnicy danych osobowych oraz znanych mi sposobów zabezpieczenia danych osobowych stosowanych przez Administratora Danych, przez cały okres zatrudnienia / świadczenia usług, jak również po ustaniu zatrudnienia / świadczenia usług.

-

-

……..……., dn. …….. …….....
(miejscowość) (data) (czytelny podpis osoby upoważnionej)

- _____

-

Wypełnia Administrator Systemów Informatycznych (ASI):

-
-
- Identyfikator/-y użytkownika:

.....

.....
(data i podpis ASI

Załącznik PODO 9

WNIOSEK O UDOSTĘPNIENIE DANYCH OSOBOWYCH

Pełna nazwa i adres administratora danych:

……
……
……
……

Pełna nazwa i adres wnioskodawcy:

……
……
……
……

Podstawa prawna udostępnienia danych osobowych:

……
……
……
……

Wskazanie przeznaczenia (cel) udostępnionych danych osobowych:

……
……
……
……

Zakres danych osobowych objętych wnioskiem:

……
……
……
……

UWAGA! Otrzymane dane mogą być wykorzystane wyłącznie do celów wskazanych we wniosku.

……

(data i podpis i ew. pieczęć wnioskodawcy)

Załącznik PODO 10

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w dniu ……. w ..... pomiędzy:

…….. z siedzibą w ……, ul. ……..., , NIP: ……..., reprezentowaną

przez: ……
zwaną dalej **Zleceniodawcą** lub **Administratorem danych (administratorem)**

a

……

zwaną dalej **Zleceniobiorcą** lub **Podmiotem przetwarzającym**
zwanymi każdą z osobna w dalszej części Umowy „**Stroną**”, a łącznie „**Stronami**”.
Zważywszy, że:

- Zleceniobiorca będzie wykonywał odpłatne świadczenie na rzecz Zleceniodawcy usług z zakresu ……..,
- Zleceniobiorca w ramach usług będzie miał dostęp do danych osobowych ……. Administratora danych,

Strony niniejszym postanawiają zawrzeć Umowę powierzenia przetwarzania danych osobowych („Umowa”), o następującej treści:

§ 1

Oświadczenia Stron

1. Przetwarzanie danych osobowych z tytułu Umowy Głównej odbywać się będzie w zgodzie i w oparciu o Rozporządzenie Parlamentu Europejskiego 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) zwanego dalej „RODO“.
2. Administrator danych powierza Zleceniobiorcy do przetwarzania dane osobowe, które zgromadził zgodnie z obowiązującymi przepisami prawa.
3. Zleceniobiorca oświadcza, że dysponuje środkami umożliwiającymi prawidłowe przetwarzanie danych osobowych powierzonych przez Administratora danych, w zakresie i celu określonym Umową.
4. Zleceniobiorca oświadcza również, że osobom zatrudnionym przy przetwarzaniu powierzonych danych osobowych nadane zostały upoważnienia do przetwarzania danych osobowych, o których mowa w art. 29 RODO oraz że osoby te zostały zapoznane z przepisami o ochronie danych osobowych oraz z odpowiedzialnością za ich nieprzestrzeganie, zobowiązały się do ich przestrzegania oraz do bezterminowego zachowania w tajemnicy przetwarzanych danych osobowych i sposobów ich zabezpieczenia.

§ 2

Cel, zakres, miejsce przetwarzania powierzonych danych osobowych

1. Administrator danych powierza Zleceniobiorcy przetwarzanie danych osobowych klientów Administratora danych jedynie w celu ……..

2. Zleceniobiorca zobowiązuje się do przetwarzania powierzonych danych osobowych wyłącznie w celach związanych z realizacją Umowy i wyłącznie w zakresie, jaki jest niezbędny do realizacji tych celów, tj. ……...
3. Na wniosek Administratora danych lub osoby, której dane dotyczą Zleceniobiorca wskaże miejsca, w których przetwarza powierzone dane.

§ 3

Zasady przetwarzania danych osobowych

1. Strony zobowiązują się wykonywać zobowiązania wynikające z niniejszej Umowy z najwyższą starannością zawodową w celu zabezpieczenia prawnego, organizacyjnego i technicznego interesów Stron w zakresie przetwarzania powierzonych danych osobowych.
2. Zleceniobiorca zobowiązuje się zastosować środki techniczne i organizacyjne mające na celu należyte, odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, zabezpieczenie

powierzonych do przetwarzania danych osobowych, w szczególności zabezpieczyć je przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów prawa, oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
3. Zleceniobiorca oświadcza, że zastosowane do przetwarzania powierzonych danych systemy informatyczne spełniają wymogi aktualnie obowiązujących przepisów prawa.
4. Zleceniobiorca przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora.
5. Podmiot przetwarzający, biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw.
6. Podmiot przetwarzający, uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (ogólne rozporządzenie o ochronie danych).
7. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora danych usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że szczególne przepisy prawa nakazują przechowywanie danych osobowych.
8. Podmiot przetwarzający udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszej umowie oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.
9. Podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody Administratora danych.

§ 4

Odpowiedzialność Stron

1. Administrator danych ponosi odpowiedzialność za przestrzeganie przepisów prawa w zakresie przetwarzania i ochrony danych osobowych według rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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. Powyższe nie wyłącza odpowiedzialności Zleceniobiorcy za przetwarzanie powierzonych danych niezgodnie z umową.
3. Podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem, jeśli nie dopełnił obowiązków, które nakłada niniejsza umowa, lub gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom.

§ 5

Postanowienia końcowe

1. Wszelkie zmiany niniejszej Umowy powinny być dokonane w formie pisemnej pod rygorem nieważności.
2. W zakresie nieuregulowanym niniejszą Umową zastosowanie mają przepisy Kodeksu cywilnego.

3. W przypadku, gdy niniejsza Umowa odwołuje się do przepisów prawa, oznacza to również inne przepisy dotyczące ochrony danych osobowych, a także wszelkie nowelizacje, jakie wejdą w życie po dniu zawarcia Umowy, jak również akty prawne, które zastąpią wskazane ustawy i rozporządzenia.
4. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.
5. Niniejsza umowa powierzenia przetwarzania danych obowiązuje na czas trwania umowy na świadczenie przez Zleceniobiorcę na rzecz Zleceniodawcy usług z zakresu obsługi windykacyjnej.

…….. ……

Zleceniodawca **Zleceniobiorca**

Załącznik PODO 11

Rejestr osób upoważnionych do przetwarzania danych osobowych

Lp.	Imię i Nazwisko	Zajmowane stanowisko	Identyfikator w systemie informatycznym*	Zakres upoważnienia do przetwarzania danych osobowych	Data nadania upoważnienia	Data ustania upoważnienia

* Identyfikator jest wymagany jeśli dane są przetwarzane w systemie informatycznym.

Załącznik PODO 12

REJESTR UDOSTĘPNIANIA DANYCH OSOBOWYCH

Lp.	Zbiór danych	Osoba Udostępniająca	Data	Podmiot, któremu udostępniono dane	Zakres Udostępnienia	Podstawa Udostępnienia

Załącznik PODO 13

WYKAZ ZBIORÓW DANYCH OSOBOWYCH

Lp.	Nazwa zbioru	Jednostka organizacyjna (departament, dział itp.)	Cel przetwarzania danych w zbiorze	Kategorie osób	Kategorie danych	Podstawa prawna upoważniająca do prowadzenia zbioru danych	Źródło danych

Załącznik PODO 14

WYKAZ OBSZARÓW PRZETWARZANIA DANYCH OSOBOWYCH

Lp.	Dokładny adres	Dział użytkujący pomieszczenie	Nr pokoju lub pomieszczenia	Rodzaj zastosowanego zabezpieczenia pomieszczenia	Uwagi

Załącznik PODO 15

REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH (art. 30 ust. 1 wg. RODO)

Dane Administratora Danych Osobowych:……., siedziba: …..... strona internetowa: ….....

Dane Inspektora Ochrony Danych: …..adres mail: …..

Data aktualizacji : ……

L. p.	Nazwa czynności przetwarzania	Dział	Cel przetwarzania (art. 30 ust.1 pkt b)	Kategorie osób (art. 30 ust. 1 pkt c)	Określenie kategorii danych (art. 30 ust. 1 pkt c)	Podstawa prawna	Źródło danych	Planowany termin usunięcia Art.. 30 ust. 1 pkt f	Nazwa współadministratora i dane kontaktowe (jeśli dotyczy) Art.. 30 ust. 1 pkt a	Nazwa podmiotu przetwarzajacego i dane kontaktowe (jeśli dotyczy) Art.. 30 ust. 1 pkt d	Kategorie odbiorców (art. 30 ust. 1 pkt d)
1,											

2,											
3,											
4,											
5,											