

Zarządzenie nr 61/2025

Wójta Gminy Zbójno

z dnia 29 sierpnia 2025 r.

zmieniające zarządzenie w sprawie wprowadzenia polityki bezpieczeństwa informacji i ochrony danych osobowych oraz polityki zarządzania systemem informatycznym w Urzędzie Gminy Zbójno

Na podstawie art. 24 ust. 2 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 95/46WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119/1 z 04 maja 2016 roku) – RODO, zarządzam co następuje:

§ 1. W zarządzeniu nr 20/2021 Wójta Gminy Zbójno z dnia 8 kwietnia 2021 r. w sprawie wprowadzenia polityki bezpieczeństwa informacji i ochrony danych osobowych oraz polityki zarządzania systemem informatycznym w Urzędzie Gminy Zbójno zmienia się załącznik nr 1, który otrzymuje brzmienie określone w załączniku do niniejszego zarządzenia.

§ 2. Zobowiązuję wszystkich pracowników Urzędu Gminy Zbójno do zapoznania się z Polityką Ochrony Danych określoną w załączniku nr 1 oraz jej stosowania.

§ 3. Wdrożenie i nadzór nad realizacją zarządzenia powierzam Inspektor Ochrony Danych Osobowych.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT

mgr Katarzyna Kukielska

Załącznik nr 1 do Zarządzenia Nr 61/2025 Wójta Gminy Zbójno z dnia 29 sierpnia 2025 r. w sprawie wprowadzenia polityki bezpieczeństwa informacji i ochrony danych osobowych oraz polityki zarządzania systemem informatycznym w Urzędzie Gminy Zbójno.

Urząd Gminy Zbójno
Zbójno 178a, 87-645 Zbójno

Kategoria informacji:	INFORMACJA JAWNA – dokument do użytku wewnętrznego
Nazwa dokumentu:	Polityka Ochrony Danych Osobowych
Identyfikator dokumentu:	PODO
Wersja dokumentu:	PODO-25/7
Data początku obowiązywania:	29.08.2025
Data końca obowiązywania:	
Zatwierdził:	Pieczęć i podpis

**POLITYKA
OCHRONY DANYCH OSOBOWYCH
W URZĘDZIE GMINY ZBÓJNO**

Zbójno
2025

§ 1 WSTĘP

1. Opracowanie i wdrożenie polityki jest obowiązkiem administratora określonym w art. 24 ust. 2 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 (Dz.Urz. UE.L.2016.119.1. z 4 maja 2016 r. oraz Dz.Urz.UE.L.2018.127.2. z 23 maja 2018 r.) – zwanego dalej jako RODO.
2. Niniejsza polityka stanowi zbiór wymogów, zasad i regulacji związanych z ochroną informacji oraz danych osobowych przetwarzanych w szczególności na podstawie:
 - 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 (Dz.Urz. UE.L.2016.119.1. z 4 maja 2016 r. oraz Dz.Urz. UE.L.2018.127.2. z 23 maja 2018 r.) (ogólne rozporządzenie o ochronie danych);
 - 2) ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz.U. z 2019 poz. 1781).
3. Przez zapewnienie ochrony danych osobowych należy rozumieć zachowanie następujących cech informacji tj.:
 - 1) poufności - daje gwarancję, że informacje są dostępne tylko dla autoryzowanych osób - pracowników, posiadających prawo dostępu do tych informacji;
 - 2) integralności - zabezpiecza ona dokładność i kompletność zarówno informacji, jak też i stosowanych metod jej ochrony oraz zapewnia, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
 - 3) dostępności - gwarancja, że użytkownicy posiadający stosowne uprawnienia mają stały dostęp do informacji i zgromadzonych zasobów;
 - 4) rozliczalności - zapewnieniu, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko jemu;
 - 5) autentyczności - zapewnieniu, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana (autentyczność dotyczy użytkowników, procesów, systemów i informacji);
 - 6) niezaprzeczalności – braku możliwości wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie;
 - 7) niezawodności – zapewnieniu spójności oraz zamierzonych zachowań i skutków, co można to interpretować jako poprawność danych i właściwa ich interpretacja.
4. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia administrator wprowadza do stosowania niniejszą politykę.
5. Politykę stosuje się w każdym podmiocie, który przetwarza wszelkie informacje i dane osobowe, w którym jest administratorem, współadministratorem lub podmiotem przetwarzającym.
6. Na bieżąco jest monitorowane ryzyko naruszenia praw lub wolności osób fizycznych, w przypadku wystąpienia okoliczności, w których mogłoby dojść do naruszenia lub utraty danych osobowych należy bez zbędnej zwłoki dokonać oceny naruszenia praw i wolności osób fizycznych. Raporty z szacowania ryzyka naruszenia praw lub wolności osób fizycznych podlegają przeglądowi raz w roku, jednak nie rzadziej, niż raz na 3 lata.
7. Doraźnego szacowania naruszenia praw lub wolności osób fizycznych dokonuje się:
 - 1) na polecenie administratora w przypadku, gdy nastąpiło naruszenie ochrony danych osobowych, którego skutkiem jest jego zgłoszenie do organu nadzorczego, zgodnie art. 33 RODO;

- 2) w przypadku powstania nowej czynności przetwarzania danych osobowych.
8. W Polityce określono techniczne i organizacyjne zabezpieczenia ochrony danych osobowych przed nieuprawnionym udostępnieniem osobom nieupoważnionym, zabranie przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy przetwarzaniu danych osobowych oraz przed zmianą, uszkodzeniem lub zniszczeniem.
9. Administrator świadomy wagi problemów związanych z ochroną prawa do prywatności, w tym w szczególności praw osób fizycznych powierzających mu swoje dane osobowe, stosuje właściwe i skuteczne metody ochrony poprzez:
- 1) podejmowanie wszelkich działań niezbędnych dla ochrony praw, wolności i usprawiedliwionych interesów jednostki związanych z ochroną osób fizycznych w związku z przetwarzaniem ich danych osobowych;
 - 2) stałe monitorowanie zagrożeń i doskonalenie stosowanych zabezpieczeń oraz przygotowanie osób przetwarzających dane osobowe w zakresie ochrony danych, w tym propagowanie świadomości wartości powierzonych danych osobowych, jako czynnika wpływającego na jakość i ciągłość działalności oraz wiarygodność administratora;
 - 3) szczególne traktowanie obowiązków pracowników w zakresie przetwarzania danych osobowych oraz stanowcze egzekwowanie ich wykonania przez zatrudnione osoby;
 - 4) doskonalenie i rozwijanie nowoczesnych metod zabezpieczenia danych przed zagrożeniami związanymi z ich przetwarzaniem, szczególnie w zakresie dotyczącym dynamicznego rozwoju metod i technik przetwarzania tych danych w systemach informatycznych oraz sieciach telekomunikacyjnych.
10. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator, także gdy występuje jako podmiot przetwarzający wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.
11. Metodyka szacowania ryzyka naruszenia praw i wolności oraz oceny skutków dla ochrony danych osobowych została określona w odrębnej dokumentacji wewnętrznej.

§ 2

PODSTAWOWE POJĘCIA

1. **RODO lub Rozporządzenie** - 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 (Dz. Urz. UE L 119 z 4 maja 2016 r., str. 1 oraz Dz. Urz. UE L 127 z 23 maja 2018 r., str. 2) – zwane dalej jako RODO;
2. **Administrator** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.
3. **Polityka ochrony danych osobowych** – dokument wewnętrzny wdrożony do użytku w organizacji przez administratora- zwany wcześniej i dalej polityką.
4. Ustanowione procedury i zasady stosuje się do wszystkich osób upoważnionych przez administratora do przetwarzania informacji w tym danych osobowych;
5. **Inspektor Ochrony Danych** – osoba wyznaczona przez administratora lub podmiot przetwarzający na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, zwany dalej inspektorem;

6. **Informatyk** – osoba wyznaczona przez administratora odpowiedzialna za sprawność i konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych do przetwarzania informacji i danych osobowych, zwany dalej informatykiem; Zadania informatyka może wykonywać także zewnętrzny podmiot w ramach umowy usługi.
7. **Podmiot przetwarzający** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
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 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;
9. **Strona trzecia** - osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;
10. **Dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
11. **Przetwarzanie** – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
12. **Ograniczenie przetwarzania** oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
13. **Profilowanie** oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
14. **Pseudonimizacja** oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.
15. **System do przetwarzania danych osobowych** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych, zwany dalej system TI;
16. **System tradycyjny** - zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji oraz wyposażenia i środków trwałych, w celu przetwarzania danych osobowych na papierze;
17. **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;

18. **Identyfikator** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
19. **Hasło** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi;
20. **Osoba upoważniona do przetwarzania danych osobowych** – rozumie się przez to osobę, upoważnioną do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający, zwana dalej upoważnionym;
21. **Użytkownik systemu** - osoba upoważniona przez administratora lub podmiot przetwarzający do przetwarzania danych osobowych, której przyznano uprawnienia do przetwarzania danych osobowych w systemie do przetwarzania danych osobowych w zakresie wskazanym w upoważnieniu, zwany dalej użytkownikiem;
22. **Naruszenie ochrony danych osobowych** oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
23. **Dane dotyczące zdrowia** oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia.

§ 3

OBZAR PRZETWARZANIA DANYCH OSOBOWYCH

1. Przetwarzanie danych osobowych w Urzędzie Gminy Zbójno odbywa się zarówno przy wykorzystaniu systemów informatycznych, jak i poza nimi, tj. w wersji tradycyjnej, „papierowej”. Obszarem przetwarzania danych osobowych jest adres: Zbójno 178a, 87-645 Zbójno.
2. Pracownicy, współpracownicy, stażyści itp. administratora, w związku z wykonywaniem swoich zadań służbowych, są upoważnieni przez administratora także do przetwarzania danych osobowych poza strefą przetwarzania wskazaną w ust. 1, przy jednoczesnym zachowaniu zasad określonych w niniejszej polityce oraz innych wewnętrznych regulacjach służących zabezpieczeniu danych osobowych;
3. Zasady zabezpieczenia fizycznego i ochrony obszarów przetwarzania danych osobowych określone zostaną w odrębnym dokumencie.

§ 4

ADMINISTRATOR

Ustala cele i sposoby przetwarzania danych, w tym zwłaszcza:

1. Jest odpowiedzialny za przestrzeganie przepisów RODO oraz niniejszej polityki uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, zarówno jako administrator i podmiot przetwarzający. Wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku:
 - 1) pseudonimizację i szyfrowanie danych osobowych,
 - 2) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
 - 3) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich, w razie incydentu fizycznego lub technicznego,

- 4) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych, mających zapewnić bezpieczeństwo przetwarzania;
2. Przeprowadza proces szacowania ryzyka naruszenia praw lub wolności osób fizycznych, w tym akceptuje ryzyko szczątkowe;
3. Przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych, w przypadku, jeśli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, kontekst i cele spowoduje wysokie ryzyko naruszenia praw lub wolności osób fizycznych;
4. Przed rozpoczęciem przetwarzania konsultuje się z organem nadzorczym, jeżeli ocena skutków dla ochrony danych, wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków, w celu zminimalizowania tego ryzyka;
5. Dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze;
6. Zawiadamia bez zbędnej zwłoki osobę, której dane dotyczą o naruszeniu ochrony danych osobowych, które może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych;
7. Zgłasza organowi nadzorczemu, bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia ochrony danych osobowych, o wystąpieniu naruszenia, jeżeli skutkuje ono ryzykiem naruszenia praw lub wolności osób fizycznych;
8. Jako podmiot przetwarzający, po stwierdzeniu każdego naruszenia ochrony danych osobowych, bez zbędnej zwłoki, zgłasza je administratorowi;
9. Upoważnia osoby fizyczne do przetwarzania danych osobowych, w tym także w przypadkach, gdy występuje jako podmiot przetwarzający.
10. Wyznacza Inspektora Ochrony Danych;
11. Zapewnia, by Inspektor Ochrony Danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych;
12. Wspiera Inspektora Ochrony Danych 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;
13. Zapewnia, by Inspektor Ochrony Danych nie otrzymywał instrukcji dotyczących wykonywania swoich zadań od innego personelu;
14. Wyznacza informatyka oraz określa zakres jego zadań i czynności;
15. Informuje każdego odbiorcę, któremu ujawniono dane osobowe, o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, chyba, że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku;
16. Współpracuje z organem nadzorczym w ramach wykonywania swoich zadań;
17. Podejmuje działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia administratora lub podmiotu przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na jego polecenie, chyba że wymaga tego od niej prawo Unii lub prawo państwa członkowskiego.
18. W przypadku powstania nowej czynności lub zmiany w czynności przetwarzania danych, jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych.

§ 5

INSPEKTOR OCHRONY DANYCH

1. Jest właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych, co zapewniają administrator oraz podmiot przetwarzający;
2. Podlega bezpośrednio administratorowi;
3. Jest zobowiązany do zachowania tajemnicy lub poufności, co do wykonywania swoich zadań;
4. Może wykonywać inne zadania i obowiązki, a administrator lub podmiot przetwarzający zapewniają, by ich wykonywanie nie powodowało konfliktu interesów;
5. Monitoruje przestrzeganie RODO i innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w zakresie ochrony danych osobowych.
6. Inicjuje i podejmuje działania, w zakresie doskonalenia bezpieczeństwa ochrony danych, prowadzi szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
7. Udziela na żądanie konsultacji, co do oceny skutków dla ochrony danych oraz monitoruje jej wykonanie;
8. Współpracuje z organem nadzorczym;
9. Pełni funkcję punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzi konsultacje we wszelkich innych sprawach;
10. Wypełnia swoje zadania z należyтым uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania;
11. Pełni funkcję punktu kontaktowego dla osób, których dane dotyczą, które mogą kontaktować się z inspektorem, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO.

§ 6

INFORMATYK

1. Informatyk realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemami oraz sieciami informatycznymi służącymi do przetwarzania danych, w tym zwłaszcza:
 - 1) Zarządza systemami oraz sieciami, w których przetwarzane są informacje i dane osobowe;
 - 2) Podejmuje działania uniemożliwiające osobom niepowołanym dostęp do systemu informatycznego, w którym przetwarzane są dane osobowe;
 - 3) Przydziela każdemu użytkownikowi identyfikator oraz hasło do systemu do przetwarzania, dokonuje modyfikacji uprawnień oraz usuwa konta użytkowników, zgodnie z zasadami określonymi w polityce;
 - 4) Podejmuje działania w zakresie ustalania i kontroli identyfikatorów dostępu do systemów informatycznych, prowadzi wykaz indywidualnych identyfikatorów przydzielonych użytkownikom;
 - 5) W uzgodnieniu z administratorem i inspektorem ochrony danych określa warunki techniczne dotyczące zabezpieczeń w systemie informatycznym;
 - 6) W sytuacji stwierdzenia naruszenia zabezpieczeń systemu do przetwarzania, w którym przetwarzane są dane osobowe informuje administratora oraz Inspektora Ochrony Danych i współdziała z nimi przy ustalaniu przyczyn i usuwaniu skutków naruszenia;
 - 7) Pisemnie dokumentuje zaistniałe incydenty bezpieczeństwa teleinformatycznego, w tym naruszenia ochrony danych osobowych oraz podjęte czynności naprawcze;
 - 8) Sprawuje nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją sprzętu informatycznego służącego do przetwarzania informacji w tym danych osobowych;

- 9) Wykonuje kopie zapasowe danych oraz dokonuje ich okresowych sprawdzeń pod kątem ich dalszej przydatności do odtwarzania danych, w przypadku awarii systemu informatycznego;
 - 10) Dokonuje systematycznego sprawdzenia wykonywania kopii zapasowych przez podmiot zewnętrzny w ramach zawartych umów;
 - 11) Podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji;
 - 12) W przypadku konieczności ujawnienia nowych czynności przetwarzania w rejestrach czynności prowadzonych przez administratora określa zabezpieczenia informatyczne, które będą miały zastosowanie przy przetwarzaniu danych;
 - 13) Bierze czynny udział w procesie analizy ryzyka m.in. poprzez czynny udział w identyfikacji zagrożeń, stosowaniu technologii informatycznych służących do zabezpieczenia danych;
 - 14) Bierze czynny udział w procesie analizy ryzyka m.in. poprzez czynny udział w identyfikacji zagrożeń, stosowaniu technologii informatycznych służących do zabezpieczenia danych.
2. Szczegółowy zakres zadań informatyka w zakresie zarządzania i bieżącego nadzoru nad systemami oraz sieciami informatycznymi służącymi do przetwarzania danych określają także inne dokumenty.
 3. W przypadku niewyznaczenia informatyka, wymienione powyżej obowiązki pełni administrator.

§ 7

OSOBA UPOWAŻNIONA DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Każda osoba fizyczna działająca z upoważnienia administratora lub podmiotu przetwarzającego, która ma dostęp do danych osobowych, przetwarza je na wyłączne polecenie administratora.
2. Z upoważnienia administratora działają:
 - 1) osoby fizyczne zatrudnione na podstawie umowy o pracę, w momencie jej zawarcia otrzymują pisemne upoważnienie - wzór zał. nr 1 do niniejszej polityki i składają oświadczenie o zachowaniu poufności – wzór zał. nr 2 do niniejszej polityki, podpisane dokumenty są włączane do akt osobowych,
 - 2) osoby fizyczne, które są stroną umowy cywilnej zawartej z administratorem, w momencie jej zawarcia uzyskują upoważnienie do przetwarzania danych osobowych zgodnie z przedmiotem umowy - wzór zał. nr 1 do niniejszej polityki i składają oświadczenie o zachowaniu poufności – wzór zał. nr 2 do niniejszej polityki, dokumenty po ich podpisaniu przekazywane są wraz z odpowiednią umową;
 - 3) osoby fizyczne, będące stażystami, wolontariuszami, innymi osobami wykonującymi czynności przetwarzania danych osobowych na rzecz administratora otrzymują upoważnienia - wzór zał. nr 1 do niniejszej polityki i składają oświadczenia o zachowaniu poufności - wzór zał. nr 2 do niniejszej polityki, dokumenty po ich podpisaniu przekazywane są wraz z odpowiednią umową;
3. Za przygotowanie w/w dokumentów oraz określenie zakresu upoważnienia odpowiada pracownik ds. kadr, inna osoba odpowiedzialna za przygotowanie umowy oraz bezpośredni przełożony;
4. Upoważnienie wygasa z momentem rozwiązania stosunku pracy, zakończenia umowy cywilnej oraz stażu, wolontariatu lub innej formy współpracy z administratorem;
5. Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana do:
 - 1) przetwarzania danych osobowych wyłącznie na polecenie administratora, zgodnie z zakresem upoważnienia, obowiązków lub umową, tylko w celu wykonywania nałożonych na nią zadań,

- 2) zachowania w tajemnicy danych osobowych, sposobów ich zabezpieczenia oraz przestrzegania procedur ich bezpiecznego przetwarzania,
- 3) przestrzegania tajemnicy danych osobowych obowiązującej przez cały okres zatrudnienia u administratora, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji, rozwiązaniu umowy i upływu terminu, na który umowa została zawarta,
- 4) zgłoszenia naruszenia ochrony danych bezpośrednio przełożonemu,
- 5) zapoznania się z przepisami prawa, aktualizowania wiedzy w zakresie ochrony danych osobowych,
- 6) stosowania określonych przez administratora procedur oraz wytycznych, mających na celu zgodne z prawem, w tym zwłaszcza adekwatne, przetwarzanie danych, określone w treści niniejszej polityki,
- 7) realizowania obowiązku informacyjnego, o którym mowa w art. 13-14 RODO,
- 8) zabezpieczenia danych przed ich udostępnianiem osobom nieupoważnionym,
- 9) niepozostawiania bez kontroli dokumentów, nośników danych i sprzętu, zwłaszcza w trakcie przenoszenia lub przetwarzania danych osobowych poza siedzibą,
- 10) zmiany hasła do systemu informatycznego w przypadku, gdy oprogramowanie nie wymusza takiego działania,
- 11) ochrony akt, zewnętrznych nośników i komputerów przenośnych,
- 12) niszczenia dokumentów w wersji papierowej oraz na nośnikach w niszczarce,
- 13) przechowywania w szafach zamykanych na klucz wszelkich wydruków zawierających dane osobowe przed opuszczeniem miejsca pracy i po zakończeniu dnia pracy,
- 14) niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych,
- 15) pisemnego zgłaszania inspektorowi wszelkich zmian otoczenia prawnego i realizowanych zadań, które powodują powstanie nowej czynności przetwarzania danych lub powodują konieczność aktualizacji rejestru czynności przetwarzania danych osobowych oraz rejestru wszystkich kategorii czynności przetwarzania,
- 16) realizowania zasad i procedur określonych w niniejszej polityce oraz innych politykach i regulaminach wprowadzonych przez administratora związanych z ochroną danych osobowych,
- 17) udzielania informacji, pomocy oraz współpracy z inspektorem ochrony danych w zakresie sprawowanej przez niego funkcji i zadań.
- 18) dokonywania dogłębnej analizy wytwarzanych dokumentów w zakresie przetwarzanych w nich danych osobowych, stosowania odpowiednich podstaw prawnych wynikających z RODO i przepisów prawa krajowego.

§ 8

REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator prowadzi rejestr czynności przetwarzania danych osobowych oraz rejestr wszystkich kategorii czynności jako podmiot przetwarzający.
2. Rejestry wymienione w ust. 1 stanowią formę dokumentowania czynności przetwarzania danych, są jednym z kluczowych elementów umożliwiających realizację zasady rozliczalności przetwarzania danych.
3. W rejestrze czynności przetwarzania danych osobowych dokumentowane są podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.
4. Ogólny opis środków służących zapewnieniu bezpieczeństwa danych osobowych stanowi załącznik do Rejestru czynności przetwarzania oraz Rejestru wszystkich kategorii czynności przetwarzania i tam podlega okresowym przeglądom i analizom.
5. Szczegółowe zasady oraz tryb postępowania przy przetwarzaniu informacji w systemach

- informatycznych określono w odrębnym dokumencie.
6. Zgłoszenia nowej czynności przetwarzania do rejestru czynności przetwarzania oraz rejestru wszystkich kategorii czynności dokonują wszystkie osoby upoważnione do przetwarzania danych osobowych przez administratora.
 7. Zgłoszenia dokonuje się niezwłocznie, nie później niż w terminie do 14 dni od wystąpienia konieczności ujawnienia nowej czynności lub kategorii czynności przetwarzania danych osobowych.
 8. Pisemny wniosek o ujawnienie nowej czynności do w/wym. rejestrów przekazywany jest do inspektora ochrony danych.
 9. Wniosek o ujawnienie nowej czynności do „Rejestru czynności przetwarzania danych osobowych administratora” stanowi wzór określony w zał. nr 3 do niniejszej polityki.
 10. Przekazanie wniosku o ujawnienie nowej czynności w „Rejestrze wszystkich kategorii czynności przetwarzania danych osobowych procesora” odbywa się poprzez przekazanie kopii lub skanu umowy powierzenia przetwarzania danych osobowych oraz innego dokumentu wskazującego administratora danych osobowych, a także zakres powierzonych zadań w ramach powierzenia lub wg wzoru określonego w zał. nr 4 do niniejszej polityki;
 11. Wniosek podpisuje osoba upoważniona lub jej przełożony.
 12. Każde ujawnienie nowej czynności w rejestrach poprzedzane jest przeprowadzeniem analizy ryzyka dla ochrony danych osobowych gdy zachodzą okoliczności określone w art. 35 RODO poddawane są ocenie skutków dla ochrony danych.
 13. Wnioski podlegają zatwierdzeniu przez administratora.
 14. Wpisu do rejestrów dokonuje inspektor ochrony danych.

§ 9

PRZETWARZANIE DANYCH OSOBOWYCH

1. Przetwarzanie odbywa się zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”);
2. Dane zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych, historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 RODO za niezgodne z pierwotnymi celami („ograniczenie celu”);
3. Gromadzone dane powinny ograniczać się do tych danych, które są niezbędne do osiągnięcia celów, w których są przetwarzane („minimalizacja danych”);
4. Dane powinny być prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość”);
5. Dane powinny być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność”);
6. Dane osobowe zbierane są od osoby, której dane dotyczą lub z innych źródeł, w granicach dozwolonych przepisami prawa;
7. Dane osobowe mogą być przetwarzane wyłącznie do realizacji celów, dla których zostały pozyskane lub powierzone;
8. Po zakończeniu przetwarzania dane należy poddać anonimizacji lub usunąć, podmiot przetwarzający po zakończeniu przetwarzania zwraca lub usuwa dane, zgodnie z decyzją administratora, oraz usuwa wszelkie ich istniejące kopie;

9. Dane winny być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane te można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 RODO, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy RODO w celu ochrony praw lub wolności osób fizycznych, których dane dotyczą („ograniczenie przechowywania”);
10. Upoważniony pracownik, zobowiązany jest w momencie zbierania danych od osoby, której dane dotyczą do spełnienia obowiązku informacyjnego oraz jeśli zachodzi taka okoliczność do odebrania zgody na przetwarzanie danych osobowych.
11. Administrator udostępnia przetwarzane dane osobowe tylko na mocy przepisów prawa lub umowy.
12. Udostępnianie danych osobowych:
 - 1) Dane osobowe mogą być udostępniane w następujących przypadkach:
 - a) na podstawie wniosku od podmiotu uprawnionego do otrzymywania danych osobowych, na podstawie przepisów,
 - b) na podstawie umowy z innym podmiotem, w ramach której istnieje konieczność udostępnienia danych,
 - c) na podstawie wniosku osoby, której dane dotyczą;
 - 2) Wniosek o udostępnienie danych osobowych musi być złożony wyłącznie w formie pisemnej pocztą tradycyjną lub elektronicznie przy użyciu profilu zaufanego lub elektronicznego podpisu kwalifikowanego i powinien zawierać informacje umożliwiające wyszukanie żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie, a w szczególności:
 - a) wnioskodawcę,
 - b) podstawę prawną upoważniającą do udostępnienia danych osobowych, ze wskazaniem konkretnego szczególnego przepisu prawa, z którego wynika obowiązek udostępniania danych,
 - c) podstawę faktyczną uzasadniającą potrzeby posiadania danych,
 - d) informacje umożliwiające przygotowanie danych do udostępnienia,
 - e) wskazanie przeznaczenia dla udostępnionych danych,
 - f) zakres danych osobowych, jakie mają być udostępnione,
 - g) datę i podpis;
 - 3) Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione;
 - 4) Wniosek o udostępnienie przekazywany jest do upoważnionego merytorycznie pracownika, odpowiedzialnego za daną czynność przetwarzania, który podejmuje decyzję o udostępnieniu danych;
 - 5) W przypadkach skomplikowanych lub merytorycznie trudnych, wniosek konsultowany jest z inspektorem ochrony danych;
 - 6) Upoważniony merytorycznie pracownik jest odpowiedzialny za przygotowanie danych osobowych do udostępnienia, w zakresie wskazanym we wniosku.

§ 10

POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

1. Powierzenie przetwarzania danych osobowych odbywa się zgodnie z art. 28 RODO, na podstawie umowy lub innego instrumentu prawnego, które wiążą podmiot przetwarzający i administratora, określając przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora;

2. Administrator korzysta wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą;
3. Upoważniony merytorycznie pracownik podejmując czynności zamierzające do zawarcia umowy na realizację usług, dostaw, robót budowlanych z podmiotami gospodarczymi, gdzie może dojść do powierzenia przetwarzania danych osobowych weryfikuje podmiot przetwarzający, ustalając czy posiada on w szczególności:
 - 1) środki wymagane na mocy art. 32 RODO,
 - 2) inspektora ochrony danych osobowych, a w przypadku braku obowiązku jego powołania inną osobę odpowiedzialną za to zagadnienie,
 - 3) politykę uwzględniającą zadania podmiotu przetwarzającego,
 - 4) rejestr czynności przetwarzania,
 - 5) rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora,Ponadto ustala:
 - 1) jeśli jest to możliwe, czy wobec podmiotu nie została wydana decyzja dotycząca naruszenia przez niego zasad przetwarzania danych,
 - 2) czy w ramach umowy powierzenia zamierza korzystać z usług innego podmiotu przetwarzającego i czy zostanie, lub została zawarta na tą okoliczność umowa powierzenia lub inny instrument prawny;
4. Weryfikacja może odbyć się z zastosowaniem „arkusza weryfikacji podmiotu przetwarzającego”, stanowiącego zał. A do wzoru umowy powierzenia przetwarzania danych osobowych, stanowiącej załącznik nr 5 do niniejszej polityki. Arkusz można wysłać do wypełnienia potencjalnemu podmiotowi przetwarzającemu lub opublikować wraz z projektem umowy powierzenia przetwarzania danych osobowych, a także wraz z ogłoszeniem o zamówieniu usługi, gdzie przewidywane jest powierzenie przetwarzania danych osobowych.
5. Ocenę zastosowanych środków technicznych i organizacyjnych zawartych w arkuszu weryfikacyjnym przeprowadza inspektor.
6. Ocenę sposobów zabezpieczania systemu informatycznego, sprzętu, programu do przetwarzania danych osobowych przeprowadza informatyk
7. Wyniki oceny zastosowanych zabezpieczeń inspektor oraz informatyk przekazują upoważnionemu merytorycznie pracownikowi w celu zawarcia umowy powierzenia lub dalszego uzupełnienia informacji zawartych w arkuszu weryfikacyjnym.
8. W przypadku konieczności przeprowadzenia audytu przed zawarciem umowy powierzenia przetwarzania danych osobowych administrator upoważnia do jego przeprowadzenia inspektora ochrony danych, informatyka, a także może skierować i upoważnić do przeprowadzenia tej czynności inne osoby posiadające odpowiednią wiedzę i doświadczenie w zakresie ochrony danych osobowych.
9. Audyt, o którym mowa wyżej dokumentowany jest w formie raportu, który zawierał będzie wnioski dotyczące zawarcia umowy powierzenia przetwarzania danych osobowych.
10. Po uzyskaniu pozytywnej weryfikacji podmiotu przetwarzającego upoważniony merytorycznie pracownik, z polecenia administratora, przygotowuje projekt umowy powierzenia dla podmiotu, który przeszedł pozytywnie proces weryfikacji określony wyżej – wzór umowy powierzenia przetwarzania danych osobowych zał. nr 6 do niniejszej polityki;
11. Upoważniony merytorycznie pracownik, odpowiedzialny za załatwienie sprawy przedkłada projekt umowy do konsultacji inspektorowi ochrony danych, a następnie do podpisu administratorowi;
12. Kopia podpisanej umowy powierzenia przetwarzania danych osobowych przekazywana jest inspektorowi.

§ 11

PRAWA OSÓB, KTÓRYCH DANE DOTYCZĄ

1. Wykonywanie praw osób.

- 1) Wniosek o realizację uprawnień przez osobę, której dane dotyczą, musi być złożony wyłącznie w formie pisemnej pocztą tradycyjną lub elektronicznie przy użyciu profilu zaufanego lub elektronicznego podpisu kwalifikowanego; pod rygorem pozostawienia wniosku bez odpowiedzi, o czym informowany jest wnioskodawca kierujący zapytanie w innej formie;
- 2) Czynności związane z realizacją uprawnień osoby, której dane dotyczą są wykonywane wyłącznie po jednoznacznym zidentyfikowaniu wnioskodawcy, że posiada prawo do danych;
- 3) Wniosek przekazywany jest do upoważnionego merytorycznie pracownika odpowiedzialnego za daną czynność przetwarzania, który poddaje analizie wniosek, biorąc pod uwagę co najmniej czy:
 - a) pochodzi od osoby uprawnionej,
 - b) administrator przetwarza dane osobowe osoby, której dane dotyczą,
 - c) czy występują przesłanki do odmowy realizacji uprawnień;
- 4) W przypadkach skomplikowanych lub merytorycznie trudnych, wniosek konsultowany jest z inspektorem ochrony danych;
- 5) Upoważniony pracownik jest odpowiedzialny za opracowanie projektu odpowiedzi i przygotowanie danych osobowych, w zakresie wskazanym we wniosku;
- 6) Decyzję o sposobie realizacji wniosku po przedłożeniu dokumentów i analizie dokonanej przez pracownika odpowiedzialnego merytorycznie podejmuje administrator;
- 7) Za opracowanie ostatecznej wersji odpowiedzi na wniosek oraz jej przesłanie odpowiedzialny jest upoważniony merytorycznie pracownik;
- 8) W przypadkach, gdy wniosek skutkuje zmianą danych osobowych w systemie informatycznym wymagającą uprawnień dostępu do danych z poziomu zarządzającego systemem informatycznym, dokonywany jest przez informatyka, po wskazaniu mu zakresu zmian jakich należy dokonać;
- 9) Udzielenie odpowiedzi na wniosek następuje w terminie do 30 dni od daty otrzymania pisemnego wniosku pochodzącego od osoby, której dane dotyczą.
- 10) Po wykonaniu w/wym. czynności, kopie dokumentów przekazywane są Inspektorowi Ochrony Danych;
- 11) Powyższe zasady stosowane są do realizacji wszystkich wniosków dot. realizacji prawa osoby, której dane dotyczą.

2. Obowiązek informacyjny

- 1) W związku z zasadą przejrzystego i jasnego komunikowania o zasadach przetwarzania, obowiązek informacyjny administratora realizowany jest w przypadkach:
 - a) bezpośredniego zbierania danych od osoby, której dane dotyczą,
 - b) pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą,
 - c) wyrażania zgody na przetwarzanie danych osobowych;
- 2) Obowiązek informacyjny jest realizowany m. in. w następujący sposób:
 - a) poprzez publikację klauzul informacyjnych na stronie www, BIP
 - b) poprzez publikację klauzul informacyjnych w siedzibie administratora,
 - c) poprzez umieszczenie stosownej klauzuli informacyjnej w dokumentach oraz jej ogłoszenie, doręczenie, przekazanie lub w inny sposób zapoznanie z jej treścią osoby, której dane dotyczą,

- d) poprzez umieszczenie odpowiednich informacji bezpośrednio w treści zgody na przetwarzanie danych osobowych,
- e) w inny sposób, przyjęty przez administratora (np. stopka w wiadomościach e-mail).

3. Prawo dostępu przysługujące osobie, której dane dotyczą

- 1) Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:
 - a) cele przetwarzania,
 - b) kategorie odnośnych danych osobowych,
 - c) o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych,
 - d) okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
 - e) o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczących osoby, której dane dotyczą oraz do wniesienia sprzeciwu wobec takiego przetwarzania,
 - f) o prawie wniesienia skargi do organu nadzorczego,
 - g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą - wszelkie dostępne informacje o ich źródle,
 - h) o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu;
- 2) Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, administrator może pobrać opłatę. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną.

4. Prawo sprostowania danych

- 1) Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe.
- 2) W przypadkach potwierdzenia konieczności zmiany posiadanych danych osobowych, pracownik:
 - a) dokonuje aktualizacji danych osobowych w posiadanej dokumentacji, w tym w systemie do przetwarzania danych osobowych,
 - b) powiadamia odbiorców, którym ujawniono dane osobowe, chyba, że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku;
 - c) informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

5. Prawo usunięcia danych „prawo bycia zapomnianym”

- 1) Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych;
- 2) Prawo usunięcia danych może nastąpić, jeżeli zachodzi jedna z przesłanek określonych w art. 17 ust. 1 RODO;
- 3) W przypadkach potwierdzenia zaistnienia przesłanek, pracownik dokonuje usunięcia danych osobowych w posiadanej dokumentacji, w tym w systemie informatycznym do przetwarzania danych osobowych;
- 4) Upoważniony merytorycznie pracownik, o usunięciu danych powiadamia odbiorców, którym ujawniono dane osobowe, chyba, że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.

- 5) informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

6. Prawo do ograniczenia przetwarzania

- 1) Osoba, której dane dotyczą, ma prawo żądania od administratora ograniczenia przetwarzania w przypadkach określonych w art. 18 RODO;
- 2) W przypadkach potwierdzenia zaistnienia przesłanek do ograniczenia przetwarzania, upoważniony merytorycznie pracownik dokonuje sprostowania danych osobowych w posiadanej dokumentacji, w tym systemie informatycznym do przetwarzania danych osobowych;
- 3) Upoważniony merytorycznie pracownik, o usunięciu danych powiadamia odbiorców, którym ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.

7. Prawo do przenoszenia danych

Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe, jeżeli:

- 1) przetwarzanie odbywa się na podstawie zgody w myśl art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) lub na podstawie umowy w myśl art. 6 ust. 1 lit. b); oraz
- 2) przetwarzanie odbywa się w sposób zautomatyzowany.
- 3) Wykonując prawo do przenoszenia danych, osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez administratora bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.
- 4) Wykonanie prawa do przenoszenia danych nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

8. Prawo do sprzeciwu

- 1) Osoba, której dane dotyczą może w dowolnym momencie wnieść do administratora sprzeciw wobec przetwarzania danych na podstawie art. 6 ust. 1 lit. e) i f) RODO. Sprzeciw nie przysługuje, w przypadku gdy :
 - a) osoba wyraziła zgodę na przetwarzanie danych. Jeżeli osoba nie chce, aby administrator dalej przetwarzał jej dane, powinna cofnąć zgodę (choć skutek może być taki sam, to z punktu widzenia prawnego sprzeciw i odwołanie zgody to konstrukcje odmienne).
 - b) podstawą przetwarzania danych osobowych jest konieczność zawarcia i realizacji umowy;
 - c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
 - d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej.
- 2) Prawo do sprzeciwu może być ograniczone także przez inne przepisy oraz obowiązki wynikające z przepisów prawa.

§ 12

POSTĘPOWANIE W PRZYPADKACH NARUSZENIA OCHRONY DANYCH OSOBOWYCH ORAZ ZGŁOSZENIE NARUSZENIA ORGANOWI NADZORCZEMU ORAZ OSOBOM, KTÓRYCH DANE DOTYCZĄ.

1. Niniejsze zasady stosuje się w przypadku:

- 1) podejrzenia naruszenia ochrony danych osobowych;

- 2) stwierdzenia naruszenia danych osobowych.
2. Charakterystyka możliwych zagrożeń:
 - 1) zagrożenia losowe zewnętrzne;
 - 2) zagrożenia losowe wewnętrzne;
 - 3) zagrożenia zamierzone, świadome i celowe.
3. Zasady postępowania opisane niżej obowiązują wszystkie osoby upoważnione do przetwarzania danych osobowych oraz pozostały personel administratora.
4. Naruszeniem ochrony danych osobowych są m.in.:
 - 1) nieuprawnione ujawnienie danych osobowych;
 - 2) przełamanie zabezpieczeń tradycyjnych – zerwane plomby na drzwiach, szafach, segregatorach;
 - 3) udostępnienie lub umożliwienie dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną;
 - 4) kradzież sprzętu komputerowego lub dokumentów zawierających dane osobowe;
 - 5) niestosowanie się do zabezpieczeń technicznych i organizacyjnych określonych w niniejszej polityce.
5. Naruszeniem ochrony danych osobowych są także zdarzenia związane z procesem przetwarzania danych osobowych przy użyciu systemu informatycznego, a w szczególności:
 - 1) nieautoryzowany dostęp do danych;
 - 2) nieautoryzowane modyfikacje lub zniszczenie danych;
 - 3) udostępnienie danych nieautoryzowanym podmiotom;
 - 4) nielegalne ujawnienie danych;
 - 5) pozyskiwanie danych z nielegalnych źródeł;
 - 6) naruszenie hasła dostępu i identyfikatora (system nie reaguje na hasło lub je ignoruje bądź można przetwarzać dane bez wprowadzenia hasła);
 - 7) częściowy lub całkowity brak danych albo dostęp do danych w zakresie szerszym niż wynikający z przyznanych uprawnień;
 - 8) braku dostępu do właściwej aplikacji lub zmiany zakresu wyznaczonego dostępu do zasobów serwera;
 - 9) „elektroniczne ślady” próby włamania do systemu informatycznego.
6. W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub zaistnienia sytuacji, które mogą wskazywać na naruszenie bezpieczeństwa danych osobowych, każdy pracownik administratora jest zobowiązany przerwać przetwarzanie danych osobowych i powiadomić o tym fakcie bezpośredniego przełożonego, a następnie postępować stosownie do podjętej przez niego decyzji.
7. Bezpośredni przełożony po uzyskaniu informacji o naruszeniu ochrony danych osobowych podejmuje działania mające na celu:
 - 1) minimalizację negatywnych skutków zdarzenia;
 - 2) wyjaśnienie okoliczności zdarzenia;
 - 3) zabezpieczenie dowodów zdarzenia;
 - 4) umożliwienie dalszego bezpiecznego przetwarzania danych.
8. Czynności w/wym. dokumentuje się w formie notatek, odbiera wyjaśnienia od pracowników oraz w innych formach umożliwiających wyjaśnienie okoliczności naruszenia.
9. O naruszeniu ochrony danych osobowych zaistniałym w związku z przetwarzaniem danych w systemie informatycznym bezpośredni przełożony informuje informatyka i inspektora.
10. Do czasu przybycia na miejsce informatyka lub upoważnionego pracownika należy:
 - 1) o ile istnieje taka możliwość, niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego zdarzenia, a następnie uwzględnić w działaniu również ustalenie jego przyczyn lub sprawców;

- 2) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej, w celu zabezpieczenia miejsca zdarzenia;
 - 3) zaniechać – o ile to możliwe – dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę incydentu;
 - 4) zastosować się do instrukcji i regulaminów lub dokumentacji aplikacji, jeśli odnoszą się one do zaistniałego przypadku;
 - 5) przygotować opis incydentu;
 - 6) nie opuszczać bez uzasadnionej przyczyny miejsca zdarzenia.
11. Informatyk lub inny pracownik wyznaczony przez administratora po otrzymaniu zawiadomienia, o którym mowa wyżej, powinien niezwłocznie:
- 1) przeprowadzić postępowanie wyjaśniające w celu ustalenia okoliczności naruszenia ochrony danych osobowych;
 - 2) podjąć działania chroniące system przed ponownym naruszeniem.
12. Informatyk, w porozumieniu z administratorem może zarządzić, w razie potrzeby, odłączenie części systemu informatycznego dotkniętej incydem od pozostałej jego części.
13. W razie odtwarzania danych z kopii zapasowych informatyk obowiązany jest upewnić się, że odtwarzane dane zapisane zostały przed wystąpieniem incydentu (dotyczy to zwłaszcza przypadków infekcji wirusowej).
14. Informatyk, ujawnienie naruszenia ochrony danych osobowych oraz czynności wykonywane w związku z naruszeniem dokumentuje, pisemną informację przekazuje bezpośredniemu przełożonemu oraz inspektorowi ochrony danych. Sporządzając pisemną informację może wykorzystać wzór „Zgłoszenia naruszenia ochrony danych osobowych” - stanowiący zał. nr 6 do niniejszej polityki.
15. Niezależnie od informatyka, osoby upoważnione oraz personel administratora, wspólnie z bezpośrednim przełożonym, w przypadku wystąpienia naruszenia ochrony danych osobowych, sporządzają pisemną informację zawierającą wszelkie informacje i ustalenia, a także przeprowadzone czynności po ujawnieniu naruszenia. Sporządzając pisemną informację mogą wykorzystać wzór „Zgłoszenia naruszenia ochrony danych osobowych” - stanowiący zał. nr 6 do niniejszej polityki.
16. Po otrzymaniu zgłoszenia o naruszeniu ochrony danych osobowych, Inspektor Ochrony Danych przeprowadza postępowanie wyjaśniające w trakcie, którego ma prawo m.in.:
- 1) żądania wyjaśnień od pracowników;
 - 2) nakazania przerwania pracy, zwłaszcza w zakresie przetwarzania danych osobowych.
17. Odmowa udzielenia wyjaśnień lub współpracy z Inspektorem Ochrony Danych traktowane będzie jako naruszenie obowiązków pracowniczych.
18. W postępowanie wyjaśniające włączeni zostają członkowie powołanego przez administratora zespołu.
19. Zespół, po zapoznaniu się z sytuacją, podjęciu czynności wyjaśniających i naprawczych przez pracowników administratora, dokonuje szacowania ryzyka utraty praw lub wolności osób fizycznych, których dane były przedmiotem naruszenia.
20. Zespół opracowuje raport końcowy – wagę naruszenia, w którym przedstawia przyczyny i skutki zdarzenia oraz wnioski, ograniczające możliwość wystąpienia zdarzenia w przyszłości, wzór raportu – wagi naruszenia określa zał. nr 7 do niniejszej polityki.
21. Raport – waga naruszenia przedstawiana jest administratorowi wraz z wnioskami dotyczącymi m.in.:
- 1) zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu;
 - 2) odstąpienia od zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu, w sytuacji, gdy jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych;
 - 3) zgłoszenia naruszenia ochrony danych osobowych administratorowi, który powierzył dane osobowe do przetwarzania;
 - 4) zawiadomienia osób, których dane dotyczą o naruszeniu ochrony danych osobowych, w przypadkach obarczonych wysokim ryzykiem naruszenia praw lub wolności osób

fizycznych oraz powiadomienia ich jakie muszą podjąć czynności, aby ograniczyć, zmniejszyć lub usunąć ryzyko naruszenia ich praw lub wolności. Zawiadomienie następuje bez zbędnej zwłoki;

- 5) wyznaczenia przez administratora pracownika, który zostanie upoważniony do udzielania informacji w zakresie naruszenia osobom, których dane były przedmiotem naruszenia;
- 6) odstąpienia od zawiadomienia osób, których dane dotyczą o naruszeniu ochrony danych osobowych w przypadku:
 - a) wdrożenia odpowiednich technicznych i organizacyjnych środków ochrony i gdy środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie,
 - b) zastosowania środków eliminujących prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
 - c) gdy wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.
- 7) określenia zagrożeń jakie zostały ujawnione w związku ze stwierdzonym naruszeniem i spowodowały jego wystąpienie.

22. Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu następuje niezwłocznie, nie później niż w ciągu 72 godzin po stwierdzeniu naruszenia.

23. Dokumentacja naruszenia zawierająca okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze przechowywana jest przez Inspektora Ochrony Danych.

§ 13

AUDYT ZGODNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH Z PRZEPISAMI O OCHRONIE DANYCH OSOBOWYCH

1. Audyty są dokonywane w formie:
 - 1) audytu planowego – według planu sprawdzeń;
 - 2) audytu doraźnego – w przypadku nieprzewidzianym w planie audytów, w sytuacji powzięcia przez administratora wiadomości o naruszeniu ochrony danych osobowych lub uzasadnionego podejrzenia wystąpienia takiego naruszenia.
2. Plan audytu określa przedmiot, zakres oraz termin przeprowadzenia poszczególnych audytów oraz sposób i zakres ich dokumentowania.
3. W planie audytu uwzględnia się, w szczególności, czynności przetwarzania danych osobowych i systemy informatyczne służące do przetwarzania danych osobowych oraz konieczność weryfikacji zgodności przetwarzania danych osobowych, z zasadami określonymi w RODO i polityce ochrony.
4. Plan audytu jest przygotowywany przez Inspektora Ochrony Danych na okres nie krótszy niż pół roku i nie dłuższy niż trzy lata.
5. Audyt doraźny jest przeprowadzany niezwłocznie po powzięciu wiadomości przez administratora o naruszeniu ochrony danych osobowych lub uzasadnionym podejrzeniu takiego naruszenia.
6. Dokumentowanie audytu może polegać, w szczególności, na utrwaleniu dowodów audytowych z systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych na informatycznym nośniku danych lub dokonaniu wydruku tych danych oraz na:
 - 1) sporządzeniu notatki z audytu, w szczególności z zebranych wyjaśnień, przeprowadzonych oględzin oraz z czynności związanych z dostępem do urządzeń, nośników oraz systemów informatycznych, służących do przetwarzania danych osobowych;
 - 2) odebraniu wyjaśnień od osoby, której czynności objęto audytem;
 - 3) sporządzeniu kopii otrzymanego dokumentu;

- 4) sporządzeniu kopii obrazu wyświetlonego na ekranie urządzenia, stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych;
- 5) sporządzeniu kopii zapisów rejestrów systemu informatycznego służącego do przetwarzania danych osobowych lub zapisów konfiguracji technicznych środków zabezpieczeń tego systemu.
7. Kluczowym elementem w trakcie audytów jest włączenie wszystkich pracowników, współpracowników administratora i ścisła współpraca z nimi, która materializuje się obowiązkiem udzielania ustnych i pisemnych wyjaśnień w zakresie prowadzonych audytów na żądanie inspektora.
8. Po zakończeniu audytu, inspektor przygotowuje raport:
 - 1) z audytu planowego – nie później niż w terminie 30 dni od jego zakończenia;
 - 2) z audytu doraźnego – niezwłocznie po zakończeniu sprawdzenia.
9. W raporcie z audytu inspektor przedstawia wnioski, rekomendacje, zalecenia z zakresu badanego obszaru.
10. Administrator po zapoznaniu się z raportem wydaje polecenia, które mają za zadanie podniesienie poziomu zapieczętowania danych osobowych oraz procesu ich przetwarzania, a także przestrzegania przepisów prawa. Wydając polecenia wskazuje osoby, których zadaniem jest ich realizacja.
11. Polecenia wydane przez administratora, inspektor ochrony danych przekazuje osobom je realizującym dokumentując ten fakt np.: podpisem na raporcie lub przesyła je pocztą elektroniczną.

§ 14

ODPOWIEDZIALNOŚĆ

1. Niezastosowanie się do niniejszej polityki i naruszenie procedur ochrony danych przez pracowników administratora może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 Kodeksu pracy.
2. Niezależnie od rozwiązania stosunku pracy, osoby popełniające przestępstwo podlegają odpowiedzialności karnej.

§ 15

RETENCJA DANYCH OSOBOWYCH

1. Administrator przetwarza dane osobowe z uwzględnieniem zasady ograniczenia przechowywania i zapewnia, że przechowuje je w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których te dane osobowe są przetwarzane (okres retencji).
2. W przypadku, gdy dla określonych danych osobowych nie występują żadne prawnie uzasadnione cele przetwarzania, administrator zaprzestaje realizowania jakichkolwiek operacji na tych danych osobowych, z wyjątkiem ich usunięcia lub nieodwracalnej anonimizacji (przez którą rozumie się modyfikację danych osobowych w taki sposób, że nie jest możliwa identyfikacja podmiotów danych).
3. W przypadkach, gdy okres retencji danych osobowych nie wynika wyraźnie z przepisów prawa, administrator ustala te okresy samodzielnie, uwzględniając ogólne zasady przetwarzania danych osobowych przewidziane w RODO. W przypadku, gdy okres retencji wynika z przepisów prawa, ma on pierwszeństwo przed postanowieniami niniejszej polityki i rejestru czynności przetwarzania.
4. Dane osobowe mogą być przetwarzane dłużej niż wynosi okres retencji, w przypadku gdy są one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych (na zasadach określonych w art. 89 ust. 1 RODO, pod warunkiem, że wdrożone są odpowiednie środki techniczne i organizacyjne w celu ochrony praw i wolności Podmiotów danych).
5. Okresy retencji danych zostały określone w jednolitym rzeczowym wykazie akt oraz rejestrze czynności przetwarzania.

6. Ustalając okresy retencji, uwzględniono w szczególności:
- 1) obowiązki prawne ciążyące na administratorze w zakresie przechowywania określonych danych osobowych lub dokumentów zawierających dane osobowe, wynikające z właściwych przepisów prawa;
 - 2) potencjalną niezbędność przetwarzania danych osobowych dla celów związanych z ustalaniem lub dochodzeniem roszczeń oraz obroną przed takimi roszczeniami i związane z tym okresy przedawnienia roszczeń wynikające z właściwych przepisów prawa.
7. Za faktyczne usuwanie (anonimizację) danych osobowych zgodnie z obowiązującymi okresami retencji odpowiedzialna jest osoba upoważniona do przetwarzania danych osobowych.
8. Przed usunięciem (anonimizacją) danych osobowych należy zweryfikować, czy nie zachodzą przesłanki wydłużenia okresu retencji, w szczególności poprzez sprawdzenie, czy:
- 1) nie występuje obowiązek prawny ciążyący na administratorze, którego wykonanie wymaga przetwarzania danych osobowych, a który nie został uwzględniony w jednolitym rzeczowym wykazie akt lub w rejestrze czynności przetwarzania;
 - 2) nie nastąpiło przerwanie lub zawieszenie okresu przedawnienia roszczeń, zgodnie z właściwymi przepisami, skutkujące koniecznością dalszego przetwarzania danych osobowych;
 - 3) dalsze przechowywanie nie jest konieczne w związku z bieżącym okresem przedawnienia zobowiązań podatkowych.
9. W razie wątpliwości przed usunięciem (anonimizacją) danych osobowych osoba upoważniona do przetwarzania danych zasięga opinii inspektora ochrony danych.
- Usunięcie (anonimizacja) danych osobowych powinno nastąpić niezwłocznie po upływie okresu retencji, z uwzględnieniem okresu koniecznego do podjęcia niezbędnych czynności technicznych i organizacyjnych związanych z usunięciem (anonimizacją) danych osobowych.

§ 16

SZKOLENIA

1. Szkoleniu podlegają wszyscy pracownicy oraz współpracownicy administratora oraz, jeśli jest to uzasadnione, pracownicy i współpracownicy podmiotów przetwarzających.
2. Niezwłocznie po otrzymaniu upoważnienia do przetwarzania danych osobowych, każdy pracownik i współpracownik przechodzą szkolenie. Szkolenie to prowadzi inspektor lub administrator oraz inne osoby posiadające odpowiednią wiedzę i umiejętności w tym zakresie.
3. O konieczności przeprowadzenia szkolenia inspektora ochrony danych powiadamia pracownik ds. kadr, inna osoba odpowiedzialna za przygotowanie umowy lub bezpośredni przełożony, z którym uzgadniania jest forma i termin szkolenia.
4. Szkolenie może odbywać się w sposób tradycyjny oraz przy użyciu środków komunikacji elektronicznej, a także informatycznych platform szkoleniowych.
5. Szkolenie dokumentowane jest listą obecności, wydrukiem z systemu informatycznego przechowywanym przez inspektora ochrony danych lub wydanym zaświadczeniem przez szkolącego. Kopia zaświadczenia przechowywana jest w aktach osobowych pracownika.
6. Każdej osobie upoważnionej do przetwarzania danych osobowych pracownik ds. kadr, inna osoba odpowiedzialna za przygotowanie umowy lub bezpośredni przełożony przedkłada przed szkolenie do zapoznania niniejszą politykę lub jej wyciąg oraz inne uregulowania wewnętrzne określające zasady ochrony i przetwarzania danych osobowych. Na tą okoliczność osoba ta składa stosowne oświadczenie, którego treść stanowi zał. 2. do niniejszej polityki - Wzór oświadczenia o zapoznaniu się z przepisami o ochronie danych osobowych.
7. Szkolenie w zakresie przetwarzania danych osobowych w systemie informatycznym przeprowadza informatyk, w momencie przekazywania identyfikatora oraz hasła przy pierwszym logowaniu się do systemu, co określają inne uregulowania wewnętrzne.

8. Szkolenia wewnętrzne wszystkich upoważnionych osób przeprowadzane są w przypadku każdej zmiany zasad lub procedur ochrony danych osobowych.
9. Szkolenie dla osób innych niż upoważnione, jest przeprowadzane, jeśli pełnione przez nie funkcje wiążą się z zabezpieczeniem danych osobowych.

§ 17

POSTANOWIENIA KOŃCOWE

1. Niniejsza polityka ma na celu zredukowanie możliwości wystąpienia negatywnych konsekwencji naruszeń w tym zakresie, tzn.:
 - 1) naruszeń danych o osobach rozumianych jako ich dobro prywatne powierzone administratorowi;
 - 2) naruszeń przepisów prawa oraz innych regulacji;
 - 3) utraty lub obniżenia reputacji administratora;
 - 4) strat finansowych, ponoszonych w wyniku nałożonych kar lub utraty wiarygodności czy klientów.
2. Polityka podlega przeglądowi i aktualizacji min. raz na trzy lata oraz w sytuacjach wystąpienia istotnych zmian w przepisach prawa związanych z ochroną danych osobowych.
3. Polityka podlega ponadto przeglądowi w sytuacji, gdy naruszenie ochrony danych osobowych nastąpiło w związku z nieaktualnymi zapisami lub błędną realizacją procedur niniejszej polityki.
4. Wzory dokumentów określone w załącznikach do polityki mogą być zastąpione innymi wzorami dokumentów jednakże zgodnymi z zasadami określonymi w RODO oraz niniejszej polityce.
5. Polityka wchodzi w życie z dniem zatwierdzenia.

Wykaz załączników:

1. Wzór upoważnienia do przetwarzania danych osobowych.
2. Wzór oświadczenia o zapoznaniu się z przepisami o ochronie danych osobowych i o zachowaniu poufności.
3. Wzór zgłoszenia nowej czynności do rejestru czynności przetwarzania danych osobowych administratora.
4. Wzór zgłoszenia nowej czynności do rejestru wszystkich kategorii czynności przetwarzania danych osobowych procesora.
5. Wzór umowy powierzenia danych osobowych do przetwarzania.
- 5a. Arkusz weryfikacji podmiotu przetwarzającego dane osobowe.
6. Wzór zgłoszenia naruszenia ochrony danych osobowych.
7. Ocena wagi naruszenia.

.....
(pieczęć jednostki)

UPOWAŻNIENIE
do przetwarzania danych osobowych

Na podstawie **art. 29 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) (Dz. Urz. UE L 119/1 z 04 maja 2016 roku) oraz w związku z:

- 1) art. 22^{1b} ustawy z dnia 26 czerwca 1974 r. Kodeks pracy*,
- 2) art. 2b ust 6 pkt 1 ustawy z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych*,
- 3) art. 8 ust. 1 b ustawy z dnia 4 marca 1994 r. o zakładowym funduszu świadczeń socjalnych*,
- 4) art. 5a pkt 2 ustawy z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji*,
- 5) inne*
- 6) inne*

Upoważniam:

.....
(imię i nazwisko)

(stanowisko)

do przetwarzania danych osobowych w **Urzędzie Gminy Zbójno** w zakresie niezbędnym do:

- 1) wykonywania określonych w zakresie obowiązków służbowych*,
- 2) realizacji umowy zlecenia*,
- 3) realizacji umowy o dzieło*,
- 3) inne*

Upoważnienia udziela się na czas pracy/wykonywania umowy zlecenia, umowy o dzieło/ praktyki/odbycia stażu/wolontariatu/.....*

.....
(data wydania upoważnienia)

.....
(pieczęć i podpis administratora)

egz. nr 1 akta osobowe

egz. nr 2 osoba upoważniona

*niepotrzebne skreślić lub wpisać wg stanu faktycznego

Załącznik nr 2 do Polityki Ochrony
Danych Osobowych

kl

Oświadczenie o zachowaniu poufności

Oświadczam, że przed rozpoczęciem wykonywania obowiązków w **Urzędzie Gminy Zbójno** zostałem/łam zapoznany/a z przepisami prawa dotyczącymi ochrony danych osobowych, 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 przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE – ogólne rozporządzenie o ochronie danych oraz z ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych, (Dz. U. 2019, poz. 1781)

Zapoznałem/łam się z Polityką Bezpieczeństwa Informacji i Ochrony Danych oraz innymi wewnętrznymi uregulowaniami określającymi ochroną i zasady przetwarzania danych osobowych. Zrozumiałem ich treść i zobowiązuję się do ich przestrzegania.

Zobowiązuję się do:

- zachowania w tajemnicy/poufności danych osobowych i innych informacji, do których mam lub będę miał/a dostęp w związku z wykonywaniem czynności zleconych w ramach stosunku pracy, również w sytuacji, gdy ustanie moja umowa obejmująca realizację tych obowiązków,
- niewykorzystywania danych osobowych w celach pozasłużbowych/ niezgodnych ze zleceniem/, umową,
- zachowania w tajemnicy/poufności informacji o sposobach zabezpieczenia danych osobowych, o ile nie są one jawne, również w sytuacji, gdy zakończę realizację moich obowiązków służbowych,
- korzystania z urządzeń technicznych oraz oprogramowania wyłącznie w związku z wykonywaniem obowiązków służbowych lub czynności zleconych przez administratora,
- należytej dbałości o wyposażenie i urządzenia techniczne.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może spowodować moją odpowiedzialność dyscyplinarną, cywilną oraz karną z art. 266 i 231 Kk.

....., dnia

.....
(podpis osoby zobowiązanej do przestrzegania zasad)

*niepotrzebne skreślić lub wpisać wg stanu faktycznego

ZATWIERDZAM

**Zgłoszenie nowej czynności do rejestru czynności przetwarzania danych osobowych
Administradora**

Nazwa czynności		
Podstawa prawna		
Cel przetwarzania danych		
Planowany termin rozpoczęcia przetwarzania danych osobowych		
Kategorie osób, których dane będą przetwarzane		
Oznaczenie rodzaju przetwarzanych danych osobowych	Dane wrażliwe*	Dane zwykłe*
Symbol JRWA lub okres przetwarzania danych		
Zakres przetwarzania danych		
Sposób przetwarzania danych osobowych	W systemie informatycznym*	W sposób tradycyjny*
Oprogramowanie wykorzystywane do przetwarzania danych osobowych		
Informatyk: wskaże sposób zabezpieczenia danych osobowych w oparciu o politykę.		
Jakim podmiotom zostaną powierzone dane do przetwarzania. Podaj ich nazwę, adres, NIP.	1. 2.	
Przygotowano projekt umowy powierzenia przetwarzania danych osobowych.	TAK*	NIE*
Sposób udostępniania danych		
Projekt klauzuli informacyjnej lub klauzuli zgody		
Uzasadnienie potrzeby wpisu czynności do rejestru		

.....
data podpis

opinia IOD:

.....
data podpis IOD

Zgłoszenie nowej czynności do rejestru wszystkich kategorii czynności przetwarzania danych osobowych procesora

Kategorie przetwarzania dokonywanych w imieniu konkretnego administratora		
Administrator (nazwa i dane kontaktowe)		
Przedstawiciel administratora		
Inspektor ochrony danych wyznaczony przez administratora (imię i nazwisko, dane kontaktowe) międzynarodowej		
Przekazywanie danych do państwa trzeciego (nazwa organizacji i dane kontaktowe) Przekazywanie danych do organizacji międzynarodowej (nazwa i dane kontaktowe) Podstawa prawna transferu danych do państwa trzeciego lub organizacji		
Kategoria danych osobowych	Dane wrażliwe*	Dane zwykłe*
Sposób przetwarzania danych osobowych	W systemie informatycznym*	W sposób tradycyjny*
Data zawarcia umowy powierzenia		
Termin obowiązywania umowy powierzenia		
Uwagi		

.....
data podpis

.....
data podpis IOD

UMOWA POWIERZENIA DANYCH OSOBOWYCH DO PRZETWARZANIA

W dniu w

pomiędzy:

reprezentowaną przez: z siedzibą w NIP,
REGON, zwaną w treść Umowy „Administratorem”

a

.....

....., ul. - reprezentowany
przez:NIP:

.....KRS,

zwaną w treść Umowy „Procesorem” lub „Przetwarzającym”,

w dalszej części Umowy Administrator i Procesor są nazywani łącznie „Stronami” lub każde oddzielenie „Stroną”

§ 1

PRZEDMIOT UMOWY

1. Strony zawarły w dniu umowę nr o świadczenie usług:, zwaną dalej „Umową usług”.
2. Mając na uwadze, że umowa wskazana powyżej dotyczy przetwarzania danych osobowych, na podstawie art. 28 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, dalej jako: „RODO”) Administrator powierzenia przetwarzania danych osobowych Procesorowi.
3. **Przetwarzanie ma charakter czasowy. Celem przetwarzania jest**
4. **Powierzenie obejmuje dane zwykłe, szczególne kategorie danych, dane wskazane w art. 10 RODO : pracowników, współpracowników, dzieci, uczniów, kontrahentów, klientów, osób kontaktujących się z administratorem, osób wyznaczonych do kontaktów, pełnomocników (itp.).**
5. Procesor uprawniony jest do przetwarzania danych osobowych wyłącznie w celu wykonania umowy określonych w ust. 1,
6. Procesor może przetwarzać powierzone mu dane osobowe dla własnych celów jedynie w przypadku dysponowania w tym zakresie odrębną podstawą prawną, o czym ma obowiązek powiadomić osoby, których dane przetwarza.

§ 2

OŚWIADCZENIA I OBOWIĄZKI PROCESORA

1. Procesor oświadcza, że posiada zasoby infrastrukturalne, doświadczenie, wiedzę oraz wykwalifikowany personel, w zakresie umożliwiającym należyte wykonanie niniejszej Umowy, w zgodzie z obowiązującymi przepisami prawa. W szczególności Procesor oświadcza, że znane mu są zasady przetwarzania i zabezpieczenia danych osobowych wynikające z RODO, których zobowiązany jest przestrzegać.
2. Procesor jest zobowiązany:
 - 1) przetwarzać powierzone dane osobowe zgodnie z RODO oraz innymi obowiązującymi przepisami prawa oraz niniejszą Umową;
 - 2) przetwarzać powierzone mu dane osobowe wyłącznie na obszarze Europejskiego Obszaru Gospodarczego (z zastrzeżeniem rozdziału 5 Umowy) oraz na urządzeniach zarządzanych przez Procesora i jego personel, z zachowaniem zasad bezpieczeństwa ochrony danych

- osobowych wymaganych przez obowiązujące przepisy prawa;
- 3) udzielać dostępu do powierzonych danych osobowych wyłącznie osobom, które ze względu na zakres wykonywanych zadań otrzymały od Procesora upoważnienie do ich przetwarzania oraz wyłącznie w celu wykonywania obowiązków wynikających z Umowy usługi;
 - 4) zapewnić, aby osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy, chyba że osoby te podlegają odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
 - 5) wdrożyć odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych, których dane osobowe będą przetwarzane na podstawie Umowy;
 - 6) wspierać Administratora w miarę możliwości, poprzez stosowanie odpowiednich środków technicznych i organizacyjnych, w realizacji obowiązku odpowiadania na żądania osób, których dane dotyczą, w zakresie wykonywania ich praw określonych w rozdziale III RODO;
 - 7) pomagać Administratorowi, uwzględniając charakter przetwarzania oraz dostępne mu informacje, wywiązać się z obowiązków określonych w art. 32-36 RODO, tj. w szczególności w zakresie:
 - a) zapewnienia bezpieczeństwa przetwarzania danych osobowych poprzez wdrożenie stosownych środków technicznych oraz organizacyjnych;
 - b) dokonywania zgłaszania naruszeń ochrony danych osobowych organowi nadzorczemu oraz zawiadamiania osób, których dane dotyczą o takim naruszeniu (obowiązki Procesora w odniesieniu do zgłaszania naruszeń zostały określone w § 8 Umowy);
 - c) przeprowadzenia przez Administratora oceny skutków dla ochrony danych oraz przeprowadzania konsultacji Administratora z organem nadzorczym;
 - 8) prowadzić, w formie pisemnej (w tym elektronicznej), rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Administratora,
 - 9) udostępniać Administratorowi, na jego uzasadnione żądanie wszelkie informacje niezbędne do wykazania spełnienia przez Administratora obowiązków wynikających z art. 28 RODO;
 - 10) umożliwić Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów, w tym inspekcji na zasadach określonych w § 6 Umowy;
 - 11) niezwłocznie informować Administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie RODO lub innych przepisów krajowych lub przepisów Unii lub państwa członkowskiego o ochronie danych;
 - 12) przechowywać dane osobowe powierzone w związku z wykonywaniem danej Umowy usługi jedynie przez okres jej obowiązywania, a także bez zbędnej zwłoki anonimizować dane lub ograniczać przetwarzanie wskazanych danych osobowych, zgodnie z wytycznymi Administratora i Umową powierzenia.

§ 3

ŚRODKI ORGANIZACYJNE I TECHNICZNE

Procesor wdraża odpowiednie środki techniczne i organizacyjne, uwzględniając stan wiedzy technicznej, koszt wdrożenia, oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku. Oceniając, czy stopień bezpieczeństwa, jest odpowiedni, Procesor uwzględnia w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub nieuzgodnionego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub

10

nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

§ 4

PODPOWIERZENIE

1. Jeżeli należyte wypełnienie obowiązków wynikających z realizacji niniejszej Umowy oraz Umowy Głównej będzie tego wymagało, Procesor może dokonać dalszego powierzenia przetwarzania danych.
2. Na dzień zawarcia niniejszej Umowy Procesor zamierza powierzyć dane osobowe następującym podmiotom, co Administrator akceptuje:
 - 1),
 - 2),
 - 3),

Na dzień zawarcie umowy Podmiot Przetwarzający w związku wykonywaniem Umowy nie powierza danych do dalszego przetwarzania podwykonawcom

3. Procesor oświadcza, że podmioty wymienione w ust. 2 spełniają wymogi, o których mowa w art. 28 Rozporządzenia i zostanie to zagwarantowane w umowach dalszego powierzenia przetwarzania danych. Uprawnienia podmiotów, którym zostanie podpowierzone przetwarzanie danych osobowych, nie mogą być szersze aniżeli uprawnienia Procesora wynikające z niniejszej Umowy.
4. Warunkiem dalszego powierzenia danych osobowych przez Procesora innym podmiotom aniżeli wymienionym w ust. 2 jest uprzednie powiadomienie Administratora drogą elektroniczną o tym fakcie, z jednoczesnym oświadczeniem Procesora, iż podmiot któremu zostaną podpowierzone dane osobowe spełnia wymogi, o których mowa w art. 28 Rozporządzenia i zostanie to zagwarantowane w umowie dalszego powierzenia przetwarzania danych. Uprawnienia podmiotu, któremu zostanie podpowierzone przetwarzanie danych osobowych, nie mogą być szersze aniżeli uprawnienia Procesora wynikające z niniejszej Umowy.
5. Administrator może sprzeciwić się dalszemu podpowierzeniu danych osobowych, w terminie 7 dni roboczych (rozumianych jako dni od poniedziałku do piątku, godz. 8.00-16.00) od otrzymania informacji, o której mowa w zdaniu poprzedzającym
6. Uprawnienie, o którym mowa w ust. 1 powyżej, nie wyłącza możliwości wyrażenia przez Administratora sprzeciwu wobec dalszego powierzenia w terminie w terminie do 7 dni roboczych (rozumianych jako dni od poniedziałku do piątku, godz. 8:00-16:00) od dnia otrzymania powiadomienia, o którym mowa w ust. 4.
7. Procesor zobowiązuje się powiadomić Administratora o rozwiązaniu lub wypowiedzeniu umowy podpowierzenia w terminie 10 dni od tego zdarzenia.

§ 5

TRANSFER DANYCH OSOBOWYCH

1. Procesor nie może przekazywać (transferować) danych osobowych do państwa trzeciego, które znajduje się poza Europejskim Obszarem Gospodarczym („EOG”), chyba że Administrator udzieli mu uprzedniej zgody zezwalającej na taki transfer.
2. Jeśli Administrator udzieli Procesorowi uprzedniej zgody na przekazanie danych osobowych do państwa trzeciego, Procesor może dokonać transferu tych danych osobowych tylko wtedy, gdy:
 - 1) państwo docelowe zapewnia adekwatny poziom ochrony danych osobowych do tego, który obowiązuje w Unii Europejskiej; lub
 - 2) Administrator i Procesor lub dalszy podmiot przetwarzający zawarli umowę w oparciu o standardowe klauzule umowne lub wdrożyli inny mechanizm, który zgodnie z przepisami prawa legalizuje transfer danych do państwa trzeciego.

§ 6

AUDYT

1. Administrator jest upoważniony do przeprowadzenia audytu zgodności z Umową oraz obowiązującymi przepisami prawa, przetwarzania przez Procesora powierzonych mu do przetwarzania danych osobowych.
2. Administrator zawiadomi Procesora o planowanym przeprowadzeniu audytu, co najmniej na 14 dni roboczych przed planowaną datą jego przeprowadzenia.
3. Jeżeli w ocenie Procesora audyt nie może zostać przeprowadzony we wskazanym terminie Procesor powinien poinformować o tym fakcie Administratora. W takim przypadku Strony wspólnie ustalą późniejszy termin audytu.
4. Audyty, o których mowa w ust. 1, mogą być wykonywane przez Administratora w miejscu przetwarzania danych osobowych objętych powierzeniem w dni robocze, w godzinach od 8:00 do 16:00. Jeżeli Administrator nie prowadzi audytu samodzielnie, może zlecić przeprowadzenie audytu jedynie podmiotom lub osobom, profesjonalnie świadczącym usługi tego rodzaju („audytor zewnętrzny”) pod warunkiem zawiadomienia, o tym Procesora z wyprzedzeniem co najmniej na 7 dni roboczych.
5. W każdym przypadku, w którym Administrator zamierza zlecić przeprowadzenie audytu, w tym inspekcji, audytorowi zewnętrznemu, Administrator ponosi odpowiedzialność za działania lub zaniechania takiego podmiotu jak za własne.
6. Administrator zobowiązany jest zapewnić, by osoby wykonujące czynności w ramach audytu, w tym audytorzy zewnętrzni, zostali zobowiązane do zachowania w poufności wszelkich informacji, które uzyskają w związku wykonywaniem audytu, a stanowiących tajemnicę przedsiębiorstwa Procesora.
7. Administrator zobowiązany jest zapewnić, by osoby wykonujące czynności w ramach audytu, w tym audytorzy zewnętrzni, nie były zatrudnione, nie były współnikami, akcjonariuszami, lub członkami organów podmiotów, wykonujących działalność konkurencyjną w stosunku do działalności prowadzonej przez Procesora, ani nie prowadzą takiej działalności konkurencyjnej we własnym imieniu.
8. Na żądanie Procesora, Administrator przedstawi w powyższym zakresie stosowne oświadczenie w formie pisemnej, pod rygorem bezskuteczności niedopuszczenia te osoby lub podmiotu do przeprowadzenia audytu. W przypadku braku złożenia tego oświadczenia, uznaje się, że wskazana osoba, w tym w audytor zewnętrzny, nie ma umocowania do przeprowadzenia audytu. Procesor będzie wówczas uprawniony do wezwania Administratora do wskazania innej osoby lub podmiotu do przeprowadzenia audytu i przedstawienia stosownego oświadczenia, dotyczącego tej osoby lub podmiotu. Do czasu wykonania tego obowiązku, Procesor będzie uprawniony do niedopuszczenia wskazanej osoby do wykonywania czynności audytowych. Postanowienia niniejsze nie naruszają uprawnienia Administratora do przeprowadzenia audytu samodzielnie.
9. Procesor, w zakresie niezbędnym do przeprowadzenia audytu, będzie współpracować z Administratorem i upoważnionymi przez niego audytorami, w szczególności zapewni im dostęp do:
 - 1) pomieszczeń i dokumentów obejmujących dane osobowe oraz informacje o sposobie przetwarzania danych osobowych,
 - 2) infrastruktury teleinformatycznej oraz systemów IT,
 - 3) osób mających wiedzę na temat procesów przetwarzania danych osobowych realizowanych przez Procesora, z uwzględnieniem konieczności zapewnienia ciągłości działalności gospodarczej i procesów biznesowych realizowanych na bieżąco przez Procesora. Administrator zapewni, że prowadzony audyt nie będzie kolidował z bieżącym wykonywaniem przez Procesora czynności w ramach prowadzonej działalności gospodarczej.
10. Po przeprowadzonym audycie Administrator sporządza protokół pokontrolny, który podpisują przedstawiciele obu Stron.

11. Koszty związane z przeprowadzeniem audytu ponosi każda ze Stron w swoim zakresie. Procesor nie jest zobowiązany do zwrotu Administratorowi jakichkolwiek kosztów związanych z wykonanym audytem, niezależnie od jego wyniku.

§ 7

POUFNOŚĆ

1. Strony mają obowiązek ochrony informacji poufnych, niezależnie od formy ich przekazania i przetwarzania, rozumianych jako informacje takie jak:
 - 1) dane osobowe, w tym szczególne kategorie danych osobowych (w rozumieniu art. 9 ust. 1 RODO),
 - 2) informacje stanowiące tajemnicę przedsiębiorstwa (w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji),
 - 3) informacje wymagające ochrony ze względu na ich znaczenie dla interesów Stron, w tym wszelkie dane techniczne, finansowe i handlowe, materiały i dokumenty,
 - 4) inne informacje bez względu na fakt, czy są one utrwalone w formie pisemnej lub w jakikolwiek inny sposób, zapisane w jakiegokolwiek formie i na jakimkolwiek nośniku, dotyczące Strony lub jej klientów, kontrahentów, dostawców, a także informacje dotyczące usług, polityki cenowej, sprzedaży, wynagrodzeń pracowników, które druga Strona otrzymała w okresie obowiązywania Umowy, lub o których dowiedziała się, czy też do których miała dostęp lub będzie w ich posiadaniu, w związku z prowadzonymi rozmowami i negocjacjami, a które nie są powszechnie znane.
2. Strony będą zwolnione z obowiązku zachowania w tajemnicy informacji poufnych w przypadku, gdy obowiązek ujawnienia informacji poufnych wynikać będzie z bezwzględnie obowiązujących przepisów prawa, bądź też prawomocnego orzeczenia lub decyzji uprawnionego sądu lub organu. O każdorazowym powzięciu informacji o takim obowiązku Strona jest zobowiązana niezwłocznie powiadomić drugą Stronę. W takim przypadku Strona zobowiązana do ujawnienia informacji poufnych będzie obowiązana do:
 - 1) ujawnienia tylko takiej części informacji poufnych, jaka jest wymagana przez prawo,
 - 2) podjęcia wszelkich możliwych działań w celu zapewnienia, iż ujawnione informacje poufne będą traktowane w sposób poufny i wykorzystywane tylko w zakresie uzasadnionym celem ujawnienia.
3. Zobowiązanie do zachowania poufności w odniesieniu do danych powierzonych w związku z daną Umową usługi jest nieograniczone w czasie.

§ 8

ZGŁASZANIE NARUSZEŃ

1. Procesor po stwierdzeniu naruszenia ochrony danych osobowych, bez zbędnej zwłoki, nie później niż w ciągu 24 godzin od stwierdzenia naruszenia, zgłasza je Administratorowi.
2. Procesor informuje o okolicznościach naruszenia i potencjalnych zagrożeniach dla ochrony powierzonych danych osobowych oraz jest zobowiązanych pisemnie określić:
 - 1) charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
 - 2) możliwe konsekwencje naruszenia ochrony danych osobowych,
 - 3) zastosowane lub proponowane środki w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków,
3. Procesor, bez zbędnej zwłoki, podejmuje wszelkie rozsądne działania mające na celu ograniczenie i naprawienie negatywnych skutków naruszenia.
4. Procesor nie jest uprawniony ani zobowiązany do powiadamiania o naruszeniu:

- 1) osób, których dane dotyczą; ani
- 2) organu nadzorczego

§ 9

CZAS TRWANIA UMOWY I ODPOWIEDZIALNOŚĆ

1. Niniejsza umowa zostaje zawarta na okres obowiązywania Umowy Głównej, o których mowa w § 1 ust. 1 z zastrzeżeniem § 9 ust. 2.
2. Administrator uprawniony jest do rozwiązania Umowy ze skutkiem natychmiastowym, w przypadku rażącego lub powtarzającego się naruszenia Umowy przez Procesora, a także w przypadku, gdy:
 - 1) organ nadzoru nad przestrzeganiem zasad przetwarzania danych osobowych stwierdzi, na podstawie prawomocnej decyzji, że Procesor lub dalszy podmiot przetwarzający nie przestrzega zasad przetwarzania danych osobowych,
 - 2) prawomocne orzeczenie sądu powszechnego wykaże, że Procesor nie przestrzega zasad przetwarzania danych osobowych – pod warunkiem uprzedniego pisemnego wezwania Procesora do zaniechania naruszeń i usunięcia ich skutków, wyznaczenia, w tym celu dodatkowego terminu, nie krótszego niż 30 dni, i bezskutecznego upływu tego terminu.
3. Administrator zobowiązuje Procesora do anonimizacji wszystkich powierzonych danych osobowych oraz usunięcia ich kopii niezwłocznie po zakończeniu obowiązywania Umowy – w terminie uzasadnionym względami technicznymi lecz w żadnym wypadku nie później niż w ciągu 30 dni, chyba że właściwe przepisy prawa krajowego lub unijnego nakazują przechowywanie tych danych osobowych. O usunięciu danych Procesor powiadomi Administratora pisemnie, w terminie 5 dni od dnia usunięcia danych, zgodnie z załącznikiem nr 1 do niniejszej umowy.
4. Procesor jest zobowiązany do podjęcia stosownego działania w celu wyeliminowania możliwości dalszego przetwarzania danych powierzonych na podstawie niniejszej Umowy.

§ 10

POSTANOWIENIA KOŃCOWE

1. Wszelka korespondencja w sprawach związanych z Umową będzie prowadzona w następujący sposób:
 - ze strony Procesora – na adres poczty elektronicznej:@......pl;
 - ze strony Administratora – na adres poczty elektronicznej:@......pl .
2. Wszelkie oświadczenia i zawiadomienia mogą być składane za pośrednictwem poczty elektronicznej, zabezpieczonej w sposób uzgodniony przez Strony, chyba że Umowa lub bezwzględnie obowiązujące przepisy prawa wymagają formy pisemnej, pod rygorem nieważności.
3. Zmiana adresów nie stanowi zmiany Umowy. O każdej zmianie danych Strony powiadomią się na piśmie, lub drogą elektroniczną, wskazując nowe dane kontaktowe.
4. Do chwili złożenia oświadczenia o zmianie danych, oświadczenia i zawiadomienia kierowane na dotychczasowe adresy uważa się za skuteczne.
5. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej Strony.
6. Zmiany Umowy są możliwe wyłącznie w formie pisemnej pod rygorem nieważności z zastrzeżeniem sytuacji, w których Umowa wprost przewiduje inną formę dokonywania zmian.
7. Użyte w Umowie pojęcia należy interpretować zgodnie z RODO.
8. Spory mające związek z Umową rozstrzygać będzie sąd właściwy dla siedziby Administratora.

Administrator

Procesor

Ve

Załącznik nr 1
do umowy powierzenia
przetwarzania danych osobowych

..... dnia,

.....
(Pełna nazwa podmiotu przetwarzającego dane)

.....
(Adres siedziby podmiotu przetwarzającego dane)

.....
(dane administratora)

Informacja o zaprzestaniu przetwarzania danych osobowych

Zgodnie z art. 28 ust. 3 lit. g rozporządzenia Parlamentu Europejskiego i Rady(UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, zwanego dalej „RODO”). Informuję, że zgodnie z Umową Powierzenia Przetwarzania Danych zawartą w dniudane osobowe przekazane przez po wygaśnięciu umowy zostały usunięte - zniszczone i nie będą wykorzystywane w dalszej działalności.

.....
(pieczęć i podpis)

Załącznik Nr 5a do Polityki Ochrony Danych

Na podstawie art. 28 ust. 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, (Dz. Urz. UE L 119 z 04.05.2016)

Przed zawarciem umowy usługi oraz powierzenia przetwarzania danych osobowych proszę o wypełnienie poniższego arkusza preaudytowego

ARKUSZ WERYFIKACJI PODMIOTU PRZETWARZAJĄCEGO DANE OSOBOWE

Lp.	Pytanie	Odpowiedź	Uwagi
1.	Czy jako podmiot przetwarzający dane osobowe planujesz wyznaczyć/wyznaczyłeś Inspektora Ochrony Danych Osobowych (IOD)?	- tak zaplanowano wyznaczenie - tak wyznaczono - nie zaplanowano wyznaczenia (uzasadnienie: np. nie jest wymagane przepisami prawa) - zaplanowano wyznaczenie (kiedy: podać przewidywaną datę)	Jeśli wyznaczyłem IOD podaj jego imię i nazwisko oraz dane kontaktowe e-mail..... tel.
2.	Jeżeli nie planuje wyznaczyć/nie został wyznaczony IOD to proszę o wskazanie innej osoby do kontaktu w kwestiach związanych z ochroną danych osobowych.	Osoba do kontaktu..., stanowisko/funkcja..., numer tel.	
3.	Czy jako podmiot przetwarzający dane osobowe wprowadziłeś środki techniczne i organizacyjne w tym politykę ochrony danych osobowych/bezpieczeństwa informacji/zarządzania systemem informatycznym, które będą spełniały wymogi RODO oraz innych aktów regulujących legalne przetwarzanie danych osobowych?	TAK/NIE	Jeśli tak np. jakie, skreśl niepotrzebne. 1. Obszar przetwarzania objęty jest zamykany/objęty ochroną/ monitoringiem wizyjnym. 2. Dostęp do stref szczególnie chronionych ograniczony jest do osób upoważnionych (serwerownia, archiwum, itp.) 3. Posiadamy niszcarki do dokumentów papierowych oraz nośników pamięci. 4. Wprowadzono politykę ochrony danych, politykę

Załącznik Nr 5a do Polityki Ochrony Danych

			zarządzania systemem informatycznym, inne regulaminy i procedury. 5. Wyznaczono osobę odpowiedzialną za ciągłość działania systemu informatycznego. 6. Pracownicy otrzymali upoważnienia do przetwarzania danych osobowych oraz odebrano od nich oświadczenie o zachowaniu danych w poufności. 7. Pracownicy posiadają aktualne uprawnienia do przetwarzania danych w systemach informatycznych. 8. Pracownicy zostali przeszkoleni w zakresie ochrony danych osobowych oraz przetwarzania danych w systemach informatycznych. 9. Tworzoną są kopie zapasowe danych. 10. Dyski twarde komputerów oraz zewnętrzne nośniki pamięci są szyfrowane. 11. Posiadamy aktualne oprogramowanie antywirusowe oraz używamy firewall. 12. Poczta elektroniczna wykorzystuje protokoły imap/pop oraz certyfikat ssl. 13. Urządzenia posiadają bieżące wsparcie oprogramowania operacyjnego. 14. Logowanie do systemów odbywa się na podstawie loginu i hasła.
--	--	--	---



Załącznik Nr 5a do Polityki Ochrony Danych

			15. Wprowadzono zasady określające złożoność haseł i jego zmian do komputerów, serwera, sieci internetowej. 16. Dostęp do sieci Wifi opatrzony jest hasłem. 17. Stosowane jest rozwiązanie „chmury obliczeniowej” 18. Przeprowadzono szacowanie ryzyka dla ochrony danych osobowych.
4.	Czy jako podmiot przetwarzający dane osobowe korzystasz z dalszych przetwarzających dane osobowe w procesie przetwarzania danych osobowych na zlecenie administratora danych osobowych?	TAK/NIE	(jeśli tak, to przygotuj wykaz tych podmiotów w celu załączenia do umowy powierzenia) 1..... 2..... 3.....
5.	Jeżeli jako podmiot przetwarzający dane osobowe korzystasz z dalszych procesorów to czy są oni zlokalizowani w ramach EOG?	TAK/NIE	
6.	Jeżeli transfer danych odbywa się poza EOG to na jakiej podstawie prawnej?	TAK/NIE	
7.	Czy z dalszymi procesorami zostały zawarte umowy powierzenia przetwarzania danych i czy stosują one środki techniczne i organizacyjne spełniające wymogi RODO?	TAK/NIE	
8.	Czy Twoi pracownicy, którzy będą przetwarzać powierzone dane, mają wydane upoważnienia do przetwarzania danych osobowych oraz odebrano od nich zobowiązanie do zachowaniu danych w poufności/tajemnicy	TAK/NIE	
9.	Czy prowadzisz rejestr czynności przetwarzania.	TAK/NIE	

Załącznik Nr 5a do Polityki Ochrony Danych

10.	Czy jako podmiot przetwarzający dane osobowe prowadzisz rejestr kategorii czynności dla powierzonych operacji przetwarzania danych osobowych?	TAK/NIE	
11.	Czy jako podmiot przetwarzający jesteś w stanie wspomagać administratora poprzez odpowiednie środki techniczne i organizacyjne, by wywiązać się z obowiązku odpowiadania na żądanie osoby, której dane dotyczą, w zakresie wykonywania jej praw?	TAK/NIE	
12.	Czy jako podmiot przetwarzający dysponujesz środkami, które pozwalają na trwałe usunięcie lub zwrot wszelkich danych osobowych oraz usunięcie ich wszelkich istniejących kopii?	TAK/NIE	Jeśli TAK to jakie są to środki? Program do usuwania danych - Niszczarka do dokumentów oraz nośników danych -.....
13.	Czy umożliwisz administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzania audytów, w tym inspekcji?	TAK/NIE	
14.	Czy jako podmiot przetwarzający dane osobowe wdrożyłeś procedury dotyczące zarządzania incydentami bezpieczeństwa?	TAK/NIE	
15.	Czy jako podmiot przetwarzający jesteś w stanie informować administratora niezwłocznie, nie później niż w ciągu 24 godzin, o naruszeniach ochrony danych osobowych, do których u Ciebie dojdzie?	TAK/NIE	
16.	Czy jako podmiot przetwarzający wprowadziłeś środki zapewniające, że systemy IT używane do przetwarzania danych osobowych są zgodne z RODO oraz innymi aktami regulującymi przetwarzanie danych osobowych?	TAK/NIE	

Załącznik Nr 5a do Polityki Ochrony Danych

17.	Czy jako podmiot przetwarzający realizujesz regularne audyty z zakresu bezpieczeństwa danych osobowych? Jeżeli tak to w jakich odstępach czasu odbywają się audyty? czy możesz udostępnić raporty?	TAK/NIE	
18.	Czy jako podmiot przetwarzający dane osobowe posiadasz aktualny certyfikat ISO 27001 /stosujesz zatwierdzony kodeks postępowania/uzyskałeś inny certyfikat/klauzulę zgodności	TAK/NIE	(jeżeli TAK wskaż właściwe)
19.	Czy wobec ciebie jako administratora lub podmiot przetwarzający została wydana decyzja dotycząca naruszenia zasad przetwarzania danych lub toczy się postępowanie związane z naruszeniem?	TAK/NIE	Jeśli TAK jakie i w jakim zakresie? Proszę podać nr decyzji UODO lub jej kopię.

*Właściwe podkreślić/uzupełnić

Podpis osoby
upoważnionej lub reprezentującej
podmiotu przetwarzający

Zgłoszenie naruszenia ochrony danych osobowych

Sporządzający zgłoszenie:

Imię i nazwisko stanowisko

Rodzaj naruszenia bezpieczeństwa danych osobowych

1. **Miejsce, dokładny czas i data ujawnienia naruszenia ochrony danych osobowych** (piętro, nr pokoju, godzina, itp.) źródło ujawnienia naruszenia:

.....
.....

2. **Opis charakteru i okoliczności naruszenia ochrony danych osobowych** (w jaki sposób doszło do naruszania, czy dotyczył danych w wersji tradycyjnej, czy elektronicznej, w tym w miarę możliwości wskazanie kategorii - wrażliwe, zwykła i zakresu danych i przybliżonej liczby osób, których dane dotyczą, oraz kategorii i przybliżonej liczby osób, których dotyczy naruszenie).

.....
.....

3. **Osoby, które uczestniczyły w zdarzeniu związanym z naruszeniem ochrony danych**

.....

4. **Działanie wskazujące na naruszenie ochrony danych osobowych:**

.....

5. **Określenie informacji mogących wskazywać na przyczynę naruszenia:**

.....

6. **Określenie wszelkich kroków podjętych po ujawnieniu naruszenia:**

.....

7. **Osoby powodujące naruszenie** (które swoim działaniem lub zaniechaniem przyczyniły się do naruszenia ochrony danych osobowych):

.....

8. **Opis możliwych konsekwencji naruszenia ochrony danych osobowych.**

.....

9. **Opis zastosowanych środków lub propozycje zastosowania środków mających na celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.**

.....

.....

10. **Zabezpieczone materiały lub inne dowody związane z wydarzeniem**

.....

.....

11. **Wnioski:**

.....

.....
(miejsce, data i godzina sporządzenia podpis
sporządzającego)

u

OCENA WAGI NARUSZENIA

W związku ze stwierdzonym w dniu r. naruszeniem ochrony danych osobowych w, dokonano oceny wagi naruszenia w celu ustalenia:

1. Czy naruszenie skutkowało ryzykiem naruszania praw lub wolności osób fizycznych?
2. Czy naruszenie podlega zgłoszeniu do Prezesa Urzędu Ochrony Danych Osobowych oraz poinformowaniu osób, których dane naruszono?
3. Czy w związku z naruszeniem należy powiadomić osoby nim objęte?
4. Jakie zagrożenia zmaterializowały się w związku ze stwierdzonym naruszeniem i spowodowały jego wystąpienie?
5. Jakiego rodzaju środki należy przedsięwziąć w celu zminimalizowania skutków naruszenia oraz zapobieżenia wystąpieniem naruszeń w przyszłości.

Zastosowano poniższą metodologię:

$$WN = KPD \times PI + ON$$

gdzie:

WN – Waga naruszenia

KPD – Kontekst Przetwarzania danych – Główny czynnik określający poziom krytyczności zestawu naruszonych danych w określonym kontekście przetwarzania

$$KPD = A + B$$

A- Rodzaj i poziom wrażliwości danych:

- 1 pkt – dane podstawowe
- 2 pkt – dane dotyczące zachowań osoby
- 3 pkt - dane finansowe
- 4 pkt – dane szczególnych kategorii

B – kontekst przetwarzania, który może podwyższyć lub obniżyć wycenę:

- Szeroki zakres danych/wolumen (+)
- Charakter danych (+/-)
- Specyfika podmiotu danych lub administratora (+/-)
- Możliwe negatywne skutki dla podmiotu danych (+)
- Publiczna dostępność danych przed naruszeniem (-)

PI - Prawdopodobieństwo identyfikacji:

- Znikome = 0,25
- Ograniczone = 0,5
- Wysokie = 0,75
- Maksymalne = 1

ON – Okoliczności naruszenia – $ON = NP + NI + ND + + IDS$

Naruszenie poufności – dane ujawnione
znanym odbiorcom danych (+0,25)

nieznanej liczbie odbiorców danych (+0,5)

Naruszenie Integralności – dane zmienione

Możliwe jest ich odzyskanie (+0,25)

Brak jest możliwości ich odzyskania (+0,5)

Naruszenie Dostępności – niedostępność danych

Czasowe (+025)

Pełna i brak możliwości ich odzyskania przez administratora lub podmiot danych (+0,5)

Intencjonalne działanie sprawcy (+0,5)

Wynik	Waga Naruszenia	Opis
WN < 2	Niska	Osoby nie zostaną dotknięte naruszeniem lub wywoła ono drobne niedogodności
2 ≤ WN < 3	Średnia	Osoby mogą napotkać niedogodności
3 ≤ WN < 4	Wysoka	Mogą wystąpić konsekwencje możliwe do pokonania, ale z poważnymi skutkami
4 ≤ WN	krytyczna	Mogą wystąpić znaczące, nawet nieodwracalne konsekwencje

Opis kontekstu naruszenia przetwarzania danych osobowych:

.....

.....

.....

Mając na względzie zaistniałe naruszenie należy przyjąć przy zastosowaniu wzoru:

$$WN = KPD \times PI + ON$$

$$KPD = A + B$$

A - Rodzaj i poziom wrażliwości danych stwierdzono, że naruszenie dotyczyło danych podstawowych, w postaci danych osobowych powiązanych z danymi finansowymi – przyjęto ... pkt.

B – po przeanalizowaniu kontekstu przetwarzania danych ustalono, że naruszenie dotyczy szerokiego zakresu danych osobowych – przyjęto ... pkt.

$$KPD = \dots \text{ pkt}$$

PI - Prawdopodobieństwo identyfikacji

Po przeprowadzaniu analizy materiałów naruszenia oraz mając na uwadze kontekst przetwarzania oraz charakter naruszonych danych ustalono, że prawdopodobieństwo identyfikacji jest na poziomie znikomym – .. pkt.

$$PI = \dots \text{ pkt}$$

$$ON - \text{Okoliczności naruszenia} - ON = NP + NI + ND + + IDS$$

Naruszenie poufności – dane ujawnione – przyjęto ... pkt.

Naruszenie Integralności – dane zmienione – przyjęto ... pkt.

Naruszenie Dostępności – niedostępność danych – przyjęto .. pkt.

Intencjonalne działanie sprawcy - z przeprowadzonych ustaleń wynika, że sprawca działa umyślnie – przyjęto + pkt.

$$ON - 0 + 0 + 0 + 0,0 = 0 \text{ pkt}$$

$$WPN = 0 \times 0 + 0 = 0$$

Waga naruszenia:

Po przeprowadzeniu analizy czynników mających wpływ na wagę naruszenia ustalono, że wynosi ona 0 pkt.

PODSUMOWANIE

W związku z zaistniałym naruszeniem osoby nim objęte mogą spotkać następujące negatywne skutki (przykłady):

- fizyczna, materialna szkoda
- szkoda niematerialna
- dyskryminacja
- kradzież tożsamości lub oszustwo dotyczące tożsamości
- nadużycia finansowe
- straty finansowe
- brak możliwości lub ograniczona możliwość zidentyfikowania osoby (np. m.in.. zmodyfikowanie, zniszczenie, utrata)
- brak możliwości lub ograniczona możliwość skorzystania z uprawnień przez podmiot danych
- nieuprawnione cofnięcie pseudonimizacji
- utrata poufności danych osobowych
- naruszenie dobrego imienia
- naruszenie dóbr osobistych
- otrzymywanie niechcianej komunikacji
- próba podszycia się pod pracownika innej instytucji w celu wyłudzenia innych danych
- poniesienie dodatkowych kosztów spowodowane np. wyłudzeniem ubezpieczenia lub środków pieniężnych z ubezpieczenia
- wykorzystanie danych do utworzenia kont w sklepach internetowych itp.
- kradzież tożsamości np. zarejestrowanie przedpłaconej karty telefonicznej
- próba wyłudzenia pożyczki bądź kredytu w instytucjach poza bankowych, przez Internet lub telefonicznie, ponieważ wiele takich instytucji umożliwia uzyskanie pożyczki lub kredytu
- w łatwy i szybki sposób bez konieczności okazywania dokumentu tożsamości
- uzyskanie przez osobę nieuprawnioną dostępu do korzystania przez nią do nieuprawnionych świadczeń, usług, dostępu do danych, pomieszczeń itp. ze świadczeń opieki zdrowotnej
- skorzystanie przez nieuprawnioną osobę z przysługujących osobom praw obywatelskich, np. udziału w głosowaniu nad środkami budżetu obywatelskiego
- zawarcia przez nieuprawnioną osobę umów cywilno-prawnych, np. najmu nieruchomości
- założeniu na przez nieuprawnioną osobę konta internetowego (np. w serwisach społecznościowych)

Należy ponadto stwierdzić, że

- jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych i **nie podlega zgłoszeniu do Prezesa Urzędu Ochrony Danych Osobowych**, ponieważ:
.....
.....
.....
.....
- nie można wykluczyć, że jest mało prawdopodobne, aby naruszenie nie poskutkowało ryzykiem naruszania praw lub wolności osoby, której dane naruszono i **podlega zgłoszeniu do Prezesa Urzędu Ochrony Danych Osobowych**

Załącznik Nr 7 do Polityki Ochrony Danych

- naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych i podlega zgłoszeniu do Prezesa Urzędu Ochrony Danych Osobowych oraz poinformowaniu osób, których dane naruszono

Na podstawie przeprowadzonego postępowania wyjaśniającego w sprawie naruszenia stwierdzono, że zmaterializowało się zagrożenie jakim jest:

-
-

Rekomendacje w celu zminimalizowania skutków naruszenia oraz zapobieżenia wystąpieniem naruszeń w przyszłości:

1. Przeprowadzenie szkolenia personelu
2.
3.

.....

.....

.....

podpisu członków zespołu

Decyzje, polecenia, uwagi administratora:

.....

.....

.....

.....

.....

.....

podpis administratora