POLITYKA OCHRONY DANYCH OSOBOWYCH W PODMIOCIE: PRZEDSZKOLE SAMORZĄDOWE "WESOŁA KRAINA" WIRY

SPIS TREŚCI

WPROWADZENIE

Celem niniejszej Polityki Ochrony Danych Osobowych (zwanej dalej: Polityka) jest opisanie zasad ochrony danych osobowych oraz dostarczenie podstawowej wiedzy z tego zakresu, w celu spełnienia wymagań 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 (zwanego dalej: RODO lub ogólne rozporządzenie o ochronie danych osobowych).

W celu zwiększenia świadomości obowiązków i odpowiedzialności osób przetwarzających dane osobowe, a tym samym skuteczności ochrony przetwarzanych zasobów, w niniejszym dokumencie opisano podstawy prawne przetwarzania danych osobowych oraz scharakteryzowano zagrożenia bezpieczeństwa, podając jednocześnie schematy postępowań na wypadek wystąpienia naruszeń.

Niniejszy dokument szczegółowo opisuje podstawowe zasady organizacji pracy przy zbiorach osobowych przetwarzanych metodami tradycyjnymi oraz w systemie informatycznym.

Dodatkowo, Polityka zawiera zestawienia w formie załączników uzupełniające treść dokumentu. Niezależnie od tego zestawienia, Administrator jest uprawniony do wprowadzania w razie potrzeby innych dokumentów (w tym wytycznych) oraz poleceń dotyczących ochrony danych osobowych. Polityka obowiązuje z dniem wydania zarządzenia. Stanowi ona jeden ze środków organizacyjnych mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z RODO.

1.REFORMA PRZEPISÓW, DEFINICJE ORAZ PODSTAWY PRAWNE

Przepisy ochrony danych osobowych zawarte są w:

- rozporządzeniu 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;
- dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW.

W dniu 25 stycznia 2012 r. Komisja Europejska przyjęła pakiet zmian reformujący prawo Unii Europejskiej w zakresie ochrony danych osobowych. Obejmował on wnioski dotyczące rozporządzenia zawierającego ogólne regulacje w zakresie ochrony danych oraz dyrektywy stanowiącej jego uszczegółowienie, dla sektora odpowiedzialnego za egzekwowanie prawa.

Porozumienie w sprawie przyjęcia nowych przepisów zostało ostatecznie osiągnięte dnia 15 grudnia 2015 r. Tym samym, główne instytucje UE: Rada Unii Europejskiej, Parlament Europejski i Komisja Europejska stworzyły zharmonizowane i nowoczesne podstawy prawne, dotyczące ochrony danych osobowych w całej Wspólnocie. Kolejnym etapem zmian było przyjecie przez Radę UE w dniu 8 kwietnia 2016 r. rozporządzenia i dyrektywy, a następnie ich zatwierdzenie przez Parlament Europejski ził dnia 14 kwietnia 2016 r.

Publikacja oficjalnych tekstów rozporządzenia i dyrektywy miała miejsce w dniu 4 maja 2016 r. w Dzienniku Urzędowym UE w językach urzędowych wszystkich państw członkowskich. Pomimo, iż datą wejścia w życie nowych regulacji (RODO) jest 24 maja 2016 r., to rozporządzenie będzie stosowane bezpośrednio od dnia 25 maja 2018 r. Dyrektywa natomiast weszła w życie z dniem 5 maja 2016 r., przy czym poszczególne państwa członkowskie UE mają czas na jej implementację do krajowego porządku prawnego najpóźniej do dnia 6 maja 2018 r.

1.1 JAKIE ZMIANY PRZYNIOSŁO RODO?

Zwiększenie ochrony danych osobowych stanowiło główny cel ogólnego rozporządzenia o ochronie danych. Akt ten doprowadził do modyfikacji dotychczasowych zasad zawartych w dyrektywie z 1995 r. Do niewątpliwych korzyści płynących z tej reformy należy zaliczyć m.in.:

- zwiększenie uprawnień przysługujących osobom fizycznym, których dane dotyczą;
- określenie ram i standardów bezpieczeństwa dostosowanych do obecnych realiów;
- wprowadzenie jednolitych przepisów w zakresie ochrony danych osobowych na terenie całej UE;
- poprawę wymiany i przepływu informacji oraz procedur wewnątrz wspólnoty;
- zwiększenie atrakcyjności rynku UE względem krajów spoza Wspólnoty.

Wprowadzone zmiany przepisów nie tylko przyczyniają się do zwiększenia kontroli osób fizycznych nad należącymi do nich danymi, ale również ułatwiają do nich dostęp. Regulacje RODO są tak skonstruowane, aby zapewnić ochronę danych osobowych wewnątrz UE, niezależnie od miejsca przetwarzania tych danych.

1.2. JAKIE KORZYŚCI DLA OSÓB FIZYCZNYCH I PODMIOTÓW PRZYNIOSŁO RODO?

RODO zapewniło różnego rodzaju środki i narzędzia służące do ochrony danych osobowych. Wśród nich możemy wymienić:

- **prawo do bycia zapomnianym** – ma na celu ochronę prywatności osób w sytuacji, w której dana osoba nie zgadza się, by informacje o niej były dalej przetwarzane, a ponadto brak jest podstawy umożliwiającej takie przetwarzanie. Instytucja ta ma za zadanie chronić prywatność osób – jej celem nie jest natomiast ułatwianie usuwania niektórych danych bądź wprowadzanie ograniczeń w zakresie wolności mediów;
- **zapewnienie łatwiejszego dostępu do danych** – ma zagwarantować osobom, których one dotyczą dostęp do szerszego kręgu informacji o przetwarzaniu danych, przy czym informacje te powinny być udostępniane w prostej i zrozumiałej formie. Instrument ten umożliwia także osobom zainteresowanym przenoszenie danych np. pomiędzy dostawcami usług internetowych;
- **obowiązek informowania o naruszeniach danych** – obliguje administratorów do zawiadomienia organu nadzorczego oraz osób, których dane dotyczą (w określonych prawem przypadkach), o naruszeniu tych danych;
- **zasadę wdrożenia mechanizmów ochrony danych w fazie projektowania (privacy by design) oraz zasadę domyślnej ochrony danych (privacy by default)** – co oznacza, że postulat ochrony danych osobowych powinien zostać uwzględniony już we wczesnym stadium np. w fazie tworzenia usługi internetowej, a standard powinny stanowić domyślne ustawienia ochrony danych osobowych gwarantujące minimalizację przetwarzanych danych;
- **zwiększoną ochronę praw dzieci** – w świetle unormowań RODO dane osobowe dzieci są przedmiotem szczególnej ochrony ze względu na fakt, że osoby małoletnie są w mniejszym stopniu świadome zagrożeń związanych z przetwarzaniem danych , jak również przysługujących im z tego tytułu praw i gwarancji.;
- **silniejsze instrumenty zapewniające egzekwowanie przepisów** – Urząd Ochrony Danych Osobowych dysponuje szerokim zakresem środków przymusu, m.in. w postaci nakładania administracyjnych kar pieniężnych, których wysokość może sięgać do 20 milionów euro lub do 4% całkowitego rocznego światowego obrotu;
- **jednolity zestaw reguł** – które dzięki RODO pozwalają na łatwiejsze i tańsze prowadzenie działalności gospodarczej w Unii Europejskiej;
- **zasada rozliczalności** – w świetle której na administratorze spoczywa ciężar udowodnienia zgodności z prawem przyjętych zasad i działań dotyczących ochrony danych osobowych;
- **ustanowienie inspektora ochrony danych** – jest obowiązkowe w przypadku organów publicznych oraz podmiotów, których działalność polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, a także danych osobowych dotyczących

wyroków skazujących i naruszeń prawa, oraz podmiotów, których główna działalność polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób. Inspektor ochrony danych, jako osoba o odpowiednich kwalifikacjach zawodowych i posiadająca niezbędną wiedzę w dziedzinie ochrony danych osobowych, ma za zadanie udzielać wsparcia w zakresie przetwarzania danych w organizacji zgodnie z RODO.

1.3 DEFINICJE

W Polityce przyjmuje się następujące definicje stosowanych pojęć: :

- **dane osobowe** oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
- **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;
- **ograniczenie przetwarzania** to oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
- **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;
- **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;
- **zbiór danych** oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
- **administrator** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę 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. Ilekroć w niniejszym dokumencie jest mowa o

administratorze należy przez to rozumieć **Przedszkole Samorządowe "Wesoła Kraina" Wiry; adres: ul. Szreniawska 4, 62-051 Wiry**

- **podmiot przetwarzający** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
- **odbiorca** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;
- **strona trzecia** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;
- **zgoda** osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne wyrażenie woli tej osoby potwierdzające, że zezwala ona na przetwarzanie danych osobowych;
- **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;
- **dane genetyczne** oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;
- **dane biometryczne** oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;
- **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;
- **przedsiębiorca** oznacza osobę fizyczną lub prawną prowadzącą działalność gospodarczą, niezależnie od formy prawnej, w tym spółki osobowe lub zrzeszenia prowadzące regularną działalność gospodarczą;
- **grupa przedsiębiorstw** oznacza przedsiębiorstwo sprawujące kontrolę oraz przedsiębiorstwa przez nie kontrolowane;

- **wiążące reguły korporacyjne** oznaczają polityki ochrony danych osobowych stosowane przez administratora lub podmiot przetwarzający, którzy posiadają jednostkę organizacyjną na terytorium państwa członkowskiego, przy jednorazowym lub wielokrotnym przekazaniu danych osobowych administratorowi lub podmiotowi przetwarzającemu w co najmniej jednym państwie trzecim w ramach grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą;
- **organ nadzorczy** oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51 RODO, w Polsce organem nadzorczym jest Urząd Ochrony Danych Osobowych;
- **organizacja międzynarodowa** oznacza organizację i organy jej podlegające działające na podstawie prawa międzynarodowego publicznego lub inny organ powołany w drodze umowy między co najmniej dwoma państwami lub na podstawie takiej umowy.

2. NAJWAŻNIEJSZE ZAGADNIENIA OCHRONY DANYCH OSOBOWYCH

2.1. PREZES URZĘDU OCHRONY DANYCH OSOBOWYCH I RADA DO SPRAW OCHRONY DANYCH OSOBOWYCH:

Prezes Urzędu Ochrony Danych Osobowych, zwany dalej „Prezesem Urzędu" – jest organem właściwym w sprawie ochrony danych osobowych.

Do jego obowiązków należy:

- prowadzenie współpracy międzynarodowej w zakresie ochrony danych,
- podejmowanie działań certyfikacyjnych i edukacyjnych,
- prowadzenie postępowań w sprawach o naruszenie przepisów o ochronie danych,
- nadzór nad wykonywaniem RODO,
- opiniowanie założeń i projektów aktów prawnych dotyczących ochrony danych osobowych,
- coroczne przedstawianie sprawozdań ze swojej działalności.

Organem opiniodawczo – doradczym Prezesa Urzędu jest Rada do Spraw Ochrony Danych Osobowych, zwana dalej „Radą".

Do zadań Rady należy:

- opiniowanie projektów dokumentów organów i instytucji Unii Europejskiej dotyczących spraw ochrony danych osobowych;
- opiniowanie przekazanych przez Prezesa Urzędu projektów aktów prawnych i innych dokumentów dotyczących spraw ochrony danych osobowych;
- opracowywanie propozycji kryteriów certyfikacji dla certyfikacji prowadzonej przez Prezesa Urzędu;
- opracowywanie propozycji rekomendacji określających środki techniczne i organizacyjne stosowane w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych;
- inicjowanie działań w obszarze ochrony danych osobowych oraz przedstawianie Prezesowi Urzędu propozycji zmian prawa w tym obszarze;
- wyrażanie opinii w sprawach przedstawionych Radzie przez Prezesa Urzędu;
- wykonywanie innych zadań zleconych przez Prezesa Urzędu.

2.2. KONTROLE URZĘDU OCHRONY DANYCH OSOBOWYCH:

Prezes Urzędu może prowadzić kontrole przestrzegania przepisów o ochronie danych osobowych, w szczególności wg następujących zasad:

- postępowanie kontrolne może być prowadzone zgodnie z zatwierdzonym przez Prezesa Urzędu planem kontroli bądź poza planem na podstawie uzyskanych przez Prezesa Urzędu informacji albo przeprowadzonych analiz;
- kontrola może być przeprowadzona przez upoważnionego pracownika Urzędu;
- do przeprowadzania kontroli Prezes Urzędu może upoważnić członka lub pracownika organu nadzorczego państwa członkowskiego Unii Europejskiej w przypadku, o którym mowa w art. 62 RODO.

W celu uzyskania informacji mogących stanowić dowód w sprawie:

- kontrolujący ma prawo wstępu na grunt oraz do budynków, lokali lub innych pomieszczeń;
- kontrolujący ma prawo wglądu do wszelkich dokumentów i wszelkich informacji mających bezpośredni związek z przedmiotem kontroli;
- kontrolujący ma prawo przeprowadzania oględzin urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania danych;
- kontrolujący może żądać złożenia pisemnych lub ustnych wyjaśnień oraz przesłuchiwać w charakterze świadka osoby w zakresie koniecznym do ustalenia stanu faktycznego;
- kontrolowany zapewnia kontrolującemu oraz osobom upoważnionym do udziału w kontroli warunki i środki niezbędne do sprawnego przeprowadzenia kontroli, a w szczególności sporządza we własnym zakresie kopie lub wydruki dokumentów oraz informacji zgromadzonych na nośnikach, w urządzeniach lub w systemach;
- kontrolowany dokonuje potwierdzenia za zgodność z oryginałem sporządzonych kopii lub wydruków. W przypadku odmowy potwierdzenia za zgodność z oryginałem potwierdza je kontrolujący, o czym czyni wzmiankę w protokole kontroli;
- w toku kontroli kontrolujący może korzystać z pomocy funkcjonariuszy innych organów kontroli państwowej lub Policji. Organy kontroli państwowej lub Policja wykonują czynności na polecenie kontrolującego;
- w uzasadnionych przypadkach przebieg kontroli lub poszczególne czynności w jej toku, po uprzednim poinformowaniu kontrolowanego, mogą być utrwalane przy pomocy urządzeń rejestrujących obraz. Informatyczne nośniki danych w rozumieniu przepisów o informatyzacji działalności podmiotów realizujących zadania publiczne, na których zarejestrowano przebieg kontroli lub poszczególne czynności w jej toku, stanowią załącznik do protokołu kontroli;
- kontrolujący może przesłuchać pracownika kontrolowanego w charakterze świadka;

- przed rozpoczęciem przesłuchania kontrolujący obowiązany jest uprzedzić świadka o odpowiedzialności karnej za zeznanie nieprawdy lub zatajenie prawdy;
- kontrolujący ustala stan faktyczny na podstawie dowodów zebranych w toku kontroli, a w szczególności dokumentów, przedmiotów, oględzin oraz ustnych lub pisemnych wyjaśnień i oświadczeń;
- przebieg przeprowadzonej kontroli kontrolujący przedstawia w protokole kontroli.

Protokół kontroli powinien zawierać:

- wskazanie nazwy albo imienia i nazwiska oraz adresu kontrolowanego;
- imię i nazwisko osoby reprezentującej podmiot kontrolowany oraz nazwę organu reprezentującego ten podmiot;
- imię i nazwisko, stanowisko służbowe, numer legitymacji służbowej oraz numer upoważnienia kontrolującego;
- datę rozpoczęcia i zakończenia czynności kontrolnych;
- określenie przedmiotu i zakresu kontroli;
- opis stanu faktycznego ustalonego w toku kontroli oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych;
- wyszczególnienie załączników;
- omówienie dokonanych w protokole poprawek, skreśleń i uzupełnień;
- informację o pouczeniu kontrolowanego o prawie zgłaszania zastrzeżeń do protokołu oraz o prawie odmowy podpisania protokołu;
- datę i miejsce podpisania protokołu przez kontrolującego i kontrolowanego.

Postępowanie kontrolne nie może trwać dłużej niż miesiąc od dnia podjęcia czynności kontrolnych. Za podjęcie czynności kontrolnych należy uznać moment, w którym kontrolujący okazuje kontrolowanemu, lub innej osobie wskazanej w przepisach, upoważnienie do przeprowadzenia kontroli oraz legitymację służbową lub inny dokument potwierdzający tożsamość.

Terminem zakończenia postępowania kontrolnego jest dzień podpisania protokołu kontrolnego przez kontrolowanego.

Jeżeli na podstawie informacji zgromadzonych w protokole kontroli Prezes Urzędu uzna, że mogło dojść do naruszenia przepisów o ochronie danych osobowych, obowiązany jest do niezwłocznego wszczęcia postępowania.

W razie stwierdzenia, że działanie lub zaniechanie wyczerpuje znamiona przestępstwa określonego w ustawie, Prezes Urzędu kieruje do organu powołanego do ścigania przestępstw zawiadomienie o popełnieniu przestępstwa, dołączając dowody dokumentujące podejrzenie.

2.3. ZGODNOŚĆ PRZETWARZANIA Z PRAWEM

Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim spełniony jest co najmniej jeden z poniższych warunków:

a) osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;

b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;

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;

e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

Lit. f) nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań.

Przetwarzanie szczególnych kategorii danych osobowych

Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby. Art. 9. ust. 1 RODO nie ma zastosowania, jeżeli spełniony jest co najmniej jeden z poniższych warunków:

- osoba, której dane dotyczą, udzieliła wyraźnej zgody na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą nie może uchylić zakazu;
- przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa

państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;

- przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;
- przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;
- przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;
- przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;
- przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;
- przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia;
- przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową;
- przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 RODO, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i

przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

2.4. PODMIOT PRZETWARZAJĄCY

- Jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.
- Podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.
- Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora. Ta umowa lub inny instrument prawny stanowią w szczególności, że podmiot przetwarzający:

  a) przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;
  b) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
  c) podejmuje wszelkie środki wymagane na mocy art. 32 RODO;
  d) biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III RODO;
  e) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36 RODO;
  f) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;
  g) udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO oraz umożliwia administratorowi lub

audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich;

h) udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich. W związku z obowiązkiem wskazanym w art. 28 ust. 3 lit. h) RODO podmiot przetwarzający niezwłocznie informuje administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie RODO lub innych przepisów Unii lub państwa członkowskiego o ochronie danych.

- Jeżeli do wykonania w imieniu administratora konkretnych czynności przetwarzania podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający nałożone zostają – na mocy umowy lub innego aktu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego – te same obowiązki ochrony danych jak w umowie lub innym akcie prawnym między administratorem a podmiotem przetwarzającym, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom RODO. Jeżeli ten inny podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec administratora za wypełnienie obowiązków tego innego podmiotu przetwarzającego spoczywa na pierwotnym podmiocie przetwarzającym.
- Wystarczające gwarancje podmiot przetwarzający może wykazać między innymi poprzez stosowanie zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 RODO lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42 RODO.
- Bez uszczerbku dla indywidualnych umów między administratorem a podmiotem przetwarzającym, umowa lub inny akt prawny, mogą się opierać w całości lub w części na standardowych klauzulach umownych, także gdy są one elementem certyfikacji udzielonej administratorowi lub podmiotowi przetwarzającemu zgodnie z art. 42 i 43 RODO.
- Bez uszczerbku dla art. 82, 83 i 84 RODO, jeżeli podmiot przetwarzający naruszy RODO przy określaniu celów i sposobów przetwarzania, uznaje się go za administratora w odniesieniu do tego przetwarzania.

W celu zapewnienia ochrony danych w przypadku powierzenia przetwarzania danych administrator podpisuje z podmiotem przetwarzającym umowy spełniające wszystkie wymogi wynikające z RODO, na przykład korzystając ze wzoru wg **załącznika nr 2**.

W celu dochowania szczególnej staranności przy wyborze procesora administrator ocenia czy podmiot mający w jego imieniu przetwarzać dane spełnia wymogi, na przykład kierując się wskazaniami wg **załącznika nr 3**.

3. ZAGROŻENIA BEZPIECZEŃSTWA

3.1. CHARAKTERYSTYKA MOŻLIWYCH ZAGROŻEŃ

- **Zagrożenia losowe zewnętrzne** - np. klęski żywiołowe, przerwy w zasilaniu, których występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, a ciągłość systemu zostaje zakłócona lecz nie dochodzi do naruszenia poufności danych;
- **Zagrożenia losowe wewnętrzne** - np. niezamierzone pomyłki operatorów, administratora systemu, awarie sprzętowe, błędy oprogramowania, przy których może dojść do zniszczenia danych, a ciągłość pracy systemu może zostać zakłócona oraz może nastąpić naruszenie poufności danych;
- **Zagrożenia zamierzone, świadome i celowe** – najpoważniejsze zagrożenia, gdzie występuje naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy). Zagrożenia te możemy podzielić na: nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych składników systemu.

3.2. SYTUACJE ŚWIADCZĄCE O NARUSZENIU ZASAD BEZPIECZEŃSTWA

- **Przełamane zabezpieczenia tradycyjne –** zerwane plomby na drzwiach, szafach, segregatorach;
- **Sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych** na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.;
- **Niewłaściwe parametry środowiska**, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych;
- **Awaria sprzętu lub oprogramowania**, które wyraźnie wskazują na umyślne działanie kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru;
- **Pojawienie się odpowiedniego komunikatu alarmowego** od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu;
- **Jakość danych w systemie** lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie;
- **Naruszenie lub próba naruszenia integralności systemu** lub bazy danych w tym systemie;
- **Próba lub modyfikacja danych** oraz zmiana w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);
- **Niedopuszczalna manipulacja** danymi osobowymi w systemie;
- **Ujawnienie osobom nieupoważnionym** danych osobowych lub objętych tajemnicą procedur ochrony przetwarzania albo innych strzeżonych elementów systemu;
- **Praca w systemie lub jego sieci komputerowej wykazująca nieprzypadkowe odstępstwa** od założonego rytmu pracy oraz wskazująca na przełamanie lub zaniechanie ochrony danych osobowych - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.;
- **Ujawnienie istnienia nieautoryzowanych kont dostępu** do danych lub tzw. „bocznej furtki", itp.;
- **Podmiana lub zniszczenie nośników z danymi osobowymi** bez odpowiedniego upoważnienia lub w sposób niedozwolony kasowania lub kopiowanie danych;
- **Rażące naruszenia dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji** (niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.).

4. INSTRUKCJA POSTĘPOWANIA Z INCYDENTAMI

Niniejsza procedura określa tryb i zasady postępowania przy przetwarzaniu danych osobowych oraz opisuje sposób reagowania na nie. Jej celem jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

4.1 TRYB POSTĘPOWANIA W PRZYPADKU NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH W SYSTEMACH INFORMATYCZNYCH

- Podmiotem odpowiedzialnym za bezpieczeństwo danych osobowych w systemach informatycznych, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe, oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie, jest administrator, korzystający z pomocy wyznaczonego przez siebie inspektora ochrony danych.
- W przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych osoba stwierdzająca naruszenie obowiązana jest niezwłocznie powiadomić o tym administratora lub inspektora ochrony danych.
- Administrator po otrzymaniu powiadomienia, w porozumieniu z inspektorem ochrony danych:
  a) podejmuje niezbędne działania mające na celu uniemożliwienie dalszego naruszenia zabezpieczenia systemu (odłączenie urządzeń, zmiana haseł);
  b) zabezpiecza, utrwala wszelkie informacje i dokumenty, które mogą stanowić pomoc przy ustaleniu przyczyn naruszenia;
  c) ustala charakter i rodzaj naruszenia oraz metody działania osób naruszających zabezpieczenie systemu;
  d) niezwłocznie przywraca prawidłowy stan działania systemu, a w przypadku uszkodzenia baz danych odtwarza je z ostatnich kopii awaryjnych z zachowaniem należytych środków ostrożności;
  e) dokonuje analizy stanu systemu wraz z oszacowaniem rozmiaru szkód powstałych na skutek naruszenia.
- Następnie administrator w porozumieniu z inspektorem ochrony danych sporządza szczegółowy raport **wg załącznika nr 4** zawierający: datę i godzinę wystąpienia incydentu, imię i nazwisko osoby powiadamiającej o zaistniałym zagrożeniu, lokalizację zdarzenia, rodzaj naruszenia bezpieczeństwa wraz z towarzyszącymi okolicznościami, przyczyny

wystąpienia naruszenia, podjęte działania, środki zaradcze oraz datę i podpis osoby sporządzającej raport.

- Następnie administrator w porozumieniu z inspektorem ochrony danych podejmuje niezbędne działania w celu zapobiegania naruszeniom zabezpieczeń systemu w przyszłości.

Jeżeli przyczyną zdarzenia był stan techniczny urządzenia, sposób działania programu, uaktywnienie się wirusa komputerowego lub jakość komunikacji w sieci telekomunikacyjnej, administrator w porozumieniu z inspektorem ochrony danych niezwłocznie przeprowadza, w stosownym zakresie, przeglądy oraz konserwacje urządzeń i programów, ustala źródło pochodzenia wirusa oraz wdraża skuteczniejsze zabezpieczenia antywirusowe, a w miarę potrzeby kontaktuje się z dostawcą usług telekomunikacyjnych.

4.2 TRYB POSTĘPOWANIA W PRZYPADKU PODEJRZENIA NARUSZENIA ZABEZPIECZEŃ DANYCH OSOBOWYCH

- Każda osoba przetwarzająca dane osobowe, w przypadku podejrzenia naruszenia zabezpieczeń danych osobowych, obowiązana jest niezwłocznie powiadomić o tym administratora lub inspektora ochrony danych.
- Administrator w porozumieniu z inspektorem ochrony danych po otrzymaniu powiadomienia (stosownie do przypuszczalnego rodzaju naruszeń):
  a) ustala zakres i przyczyny incydentu oraz jego ewentualne skutki;
  b) inicjuje ewentualne działania dyscyplinarne;
  c) działa na rzecz przywrócenia działań organizacji po wystąpieniu incydentu;
  d) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia.
- W przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych administrator w porozumieniu z inspektorem ochrony danych:
  a) podejmuje niezbędne działania mające na celu uniemożliwienie dalszego ich naruszenia;
  b) zabezpiecza, utrwala wszelkie informacje i dokumenty mogące stanowić pomoc przy ustaleniu przyczyn naruszenia;
  c) dokonuje analizy stanu zabezpieczeń wraz z oszacowaniem rozmiaru szkód powstałych na skutek ich naruszenia;
  d) sporządza szczegółowy raport zawierający w szczególności: datę i godzinę otrzymania informacji o naruszeniu, opis jego przebiegu, przyczyny oraz wnioski ze zdarzenia.
- Następnie administrator w porozumieniu z inspektorem ochrony danych sporządza szczegółowy raport **wg załącznika nr 4** zawierający: datę i godzinę wystąpienia incydentu, imię i nazwisko osoby powiadamiającej o zaistniałym zagrożeniu, lokalizację zdarzenia, rodzaj naruszenia bezpieczeństwa wraz z towarzyszącymi okolicznościami, przyczyny wystąpienia naruszenia, podjęte działania, środki zaradcze oraz datę i podpis osoby sporządzającej raport.
- Administrator w porozumieniu z inspektorem ochrony danych podejmuje niezbędne działania w celu zapobiegania naruszeniom zabezpieczeń systemu w przyszłości.

Tabela opisująca przykładowe zagrożenia oraz sposoby postępowania w przypadku naruszeń bezpieczeństwa danych osobowych

RODZAJ NARUSZENIA	WYTYCZNE DOTYCZĄCE POSTĘPOWANIA
DOTYCZĄCE WIEDZY	
Ujawnianie danych dotyczących sprzętu i środowiska informatycznego.	Należy niezwłocznie przerwać rozmowę bądź inną czynność zmierzającą do ujawnienia informacji. Powiadomić zgodnie z procedurą. Przygotować raport z opisem dotyczącym, informacji, która została ujawniona.
Ujawnianie sposobu działania aplikacji i systemu oraz zabezpieczeń osobom niepowołanym.	
Dopuszczanie i stwarzanie warunków, aby jakikolwiek podmiot taką wiedzę mógł pozyskać np. na podstawie obserwacji lub dokumentacji.	
DOTYCZĄCE OPROGRAMOWANIA I SPRZĘTU	
Umożliwienie korzystania ze sprzętu i oprogramowania komputerowego wraz z dostępem do bazy danych osobom nieuprawnionym.	Należy określić zakres czynności, które zostały wykonane przez osobę nieuprawnioną, a następnie wezwać taką osobę do niezwłocznego opuszczenia stanowiska. W dalszej kolejności należy dokonać zawiadomienia zgodnie z procedurą oraz sporządzić raport.
Umożliwienie korzystania z aplikacji zapewniającej dostęp do bazy danych osobowych przez osoby nieupoważnione	Należy wezwać osobę bezprawnie korzystającą z aplikacji do niezwłocznego zaprzestania korzystania i opuszczenia stanowiska komputerowego. Następnie, należy pouczyć osobę odpowiedzialną za dopuszczenie do takiej sytuacji. Powiadomienie zgodnie z przyjętą procedurą i sporządzenie raportu.
Pozostawienie niezabezpieczonego hasła dostępu do bazy danych osobowych lub sieci, np. w ogólnodostępnym lub widocznym miejscu	Należy niezwłocznie zabezpieczyć dane z hasłami tak, aby uniemożliwić ich odczyt. Zawiadomienie zgodnie z obowiązującą procedurą oraz sporządzenie raportu.
Pozostawienie stanowiska pracy z działającym oprogramowaniem umożliwiającym dostęp do bazy danych osobowych.	Należy natychmiast przerwać działanie aplikacji oraz dokonać zawiadomienia zgodnie z obowiązującą procedurą, a następnie sporządzić raport.
Samowolne instalowanie oprogramowania.	Należy wezwać osobę wykonującą takż czynność do jej zaniechania, a następnie

	powiadomić personel działu informatycznego, w celu odinstalowania oprogramowania. W dalszej kolejności konieczne jest powiadomienie wg przyjętych procedur oraz sporządzenie raportu.
Korzystanie z nośników (np. dyski zewnętrzne USB) bez uprzedniego sprawdzenia ich zawartości oprogramowaniem antywirusowym.	Należy poinformować osobę dopuszczającą się takich działań o ich szkodliwości i możliwych następstwach, a następnie zlecić działowi informatycznemu wykonanie kontroli antywirusowej. Standardowo należy również powiadomić zgodnie z procedurami oraz przygotować raport.
Samowolna ingerencja w parametry systemu i oprogramowanie.	Należy wezwać osobę, aby niezwłocznie zaprzestała dokonywać takich działań. Dokonać zawiadomienia zgodnie z procedurami i sporządzić raport.
DOTYCZĄCE DOKUMENTÓW ZAWIERAJĄCYCH DANE OSOBOWE	
Kopiowanie dokumentacji oraz utrata kontroli nad wykonaną kopią.	Należy niezwłocznie zaniechać powielania i dokonać zabezpieczenia wykonanej kopii. Następnie należy zawiadomić wedle przyjętych procedur oraz sporządzić raport.
Niewłaściwe zabezpieczenie dokumentów podczas ich przechowywania, umożliwiające do nich dostęp osobom nieuprawnionym.	Konieczne jest poinformowanie przełożonych oraz dokonanie powiadomienia wg przyjetej procedury i wykonanie raportu.
Niszczenie dokumentów w sposób umożliwiający odczytanie zawartej w nich treści.	Należy dokonać zabezpieczenia niewłaściwie zniszczonych dokumentów, a następnie powiadomić zgodnie z procedurą i sporządzić raport.
Pozostawienie dokumentów bez nadzoru w otwartych pomieszczeniach.	Należy niezwłocznie zabezpieczyć dokumenty, dokonać powiadomienia wg przyjętej procedury oraz sporządzić raport.
Umożliwienie osobom trzecim odczytanie zawartości ekranu komputerowego, na którym znajdują się dane osobowe.	Należy niezwłocznie wezwać osobę dopuszczającą się tych czynności do ich zaprzestania oraz wyłączyć monitor lub komputer. Następnie należy dokonać zawiadomienia wg obowiązującej procedury oraz w przypadku wycieku istotnych danych przygotować raport
Pozbawienie kontroli nad kopią dokumentu zawierającego dane osobowe.	Należy podjąć niezbędne kroki celem odzyskania kopii utraconego dokumentu, a

	następnie powiadomić wg przyjętej procedury i przygotować raport.
Wykonanie kopii danych na nośniku w sytuacjach nie objętych procedurą.	Należy niezwłocznie zakończyć proces kopiowania danych oraz podjąć próbę zabezpieczenia egzemplarza wykonanej kopii. Następnie należy zawiadomić wg procedury oraz sporządzić raport.
DOTYCZĄCE POMIESZCZEŃ I INFRASTRUKTURY, W TYM SIECI KOMPUTEROWYCH, PRZEZNACZONYCH DO PRZETWARZANIA DANYCH	
Umożliwianie dostępu do pomieszczeń i znajdującego się w nich sprzętu (komputery) osobom nieuprawnionym lub nieznanym.	Należy wezwać takie osoby do niezwłocznego opuszczenia pomieszczeń oraz podjąć działania w celu ustalenia ich tożsamości. Następnie należy dokonać powiadomienia wg procedury oraz sporządzić raport.
Pozostawianie bez dozoru lub opuszczenie niezamkniętego pomieszczenia, w którym znajduje się sprzęt komputerowy, na którym przetwarzane są dane osobowe, umożliwiając w ten sposób ingerencję w sprzęt lub oprogramowanie osobom nieuprawnionym.	W pierwszej kolejności należy zabezpieczyć pomieszczenie, w którym znajduje się sprzęt, a następnie powiadomić zgodnie z przyjętą procedurą i sporządzić raport.
Zezwolenie osobom do tego nieuprawionym na ingerencję w sieć komputerową, w tym na podłączanie urządzeń do sieci komputerowej, demontaż lub modyfikowanie elementów infrastruktury sieci komputerowej.	Należy zidentyfikować oraz wezwać osoby dopuszczające się wskazanych czynności do ich natychmiastowego zaprzestania, a następnie powiadomić zgodnie z procedurą i sporządzić raport.
Umożliwianie osobom nieuprawnionym dokonywanie ingerencji w urządzenia sieci komputerowej znajdującej się w miejscach dostępnych publicznie (korytarze, klatki schodowe, hol itp.).	Należy niezwłocznie zidentyfikować oraz wezwać osoby dopuszczające się opisanych naruszeń do ich zaniechania oraz opuszczenia pomieszczeń. Następnie trzeba powiadomić według przyjętej procedury oraz sporządzić raport.
Umożliwianie osobom nieuprawnionym dostępu do pomieszczeń, w których znajdują się serwery i komputery centralne	Należy niezwłocznie zidentyfikowac i wezwać osoby dokonujące opisanych czynność do ich zaniechania i opuszczenia pomieszczeń, a następnie zawiadomić zgodnie z procedurą i sporządzić raport.

Wykaz potencjalnych zjawisk i symptomów wskazujących na naruszenie ochrony danych osobowych

<table>
<tr><th>RODZAJE NARUSZEŃ</th><th>REKOMENDOWANE DZIAŁANIA</th></tr>
<tr><td>Oznaki włamania do pomieszczeń, gdzie przetwarzane są dane osobowe.</td><td>Należy podjąć działania stosownie do obowiązujących przepisów (zawiadomienie organów ścigania), dokonać zawiadomienia według przyjętej procedury oraz sporządzić raport.</td></tr>
<tr><td>Zmieniony wygląd i działanie aplikacji służących do przetwarzania danych.</td><td rowspan="3">Należy niezwłocznie poinformować dział informatyczny, jak również zaprzestać korzystania ze sprzętu i oprogramowania. Powiadomienie powinno zostać dokonane zgodnie z procedurą. Wymagane jest sporządzenie raportu.</td></tr>
<tr><td>Nagłe i niespodziewane, zmiany zawartości bazy danych.</td></tr>
<tr><td>Obecność nowego oprogramowania, sprzętu nieznanego pochodzenia lub wystąpienie innych zmian w systemach lub konfiguracji oprogramowania.</td></tr>
<tr><td>Oznaki świadczące o ingerencji lub manipulacji w infrastrukturę sieci komputerowych lub sprzęt</td><td>Należy natychmiast powiadomić odpowiednie służby, w tym informatyczne oraz zaprzestać używania sprzętu lub oprogramowania do momentu wyjaśnienia sytuacji. Następnie należy dokonać zawiadomienia zgodnie z obowiązującą procedurą oraz przygotować raport.</td></tr>
</table>

Wykaz sposobów naruszeń ochrony danych osobowych przez służby informatyczne w ramach pomocy technicznej udzielanej użytkownikom

<table>
<tr><th>RODZAJE NARUSZEŃ</th><th>REKOMENDOWANE DZIAŁANIA</th></tr>
<tr><td>Prośba o udostępnienie haseł umożliwiających dostęp do danych osobowych w ramach wsparcia technicznego.
Nieuprawnione przeglądanie lub ingerowanie w dane osobowe użytkownika (w ramach wsparcia technicznego), przy wykorzystaniu loginu i hasła użytkownika</td><td>Należy, dokonać powiadomienia zgodnie z przyjętą procedurą, a następnie sporządzić raport.</td></tr>
</table>

4.3 NOTYFIKACJA NARUSZEŃ

W przypadku naruszenia ochrony danych osobowych administrator zgłasza je Prezesowi Urzędu Ochrony Danych Osobowych. Jednak nie ma obowiązku zgłoszenia, jeżeli jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Administrator dokonuje samodzielnej oceny, czy zaistniałą sytuację objął obowiązek zgłoszenia. Następne bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je Prezesowi Urzędu Ochrony Danych Osobowych o ile naruszenie skutkuje ryzykiem naruszenia prawa lub wolności osób fizycznych. Do zgłoszenia przekazanego po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

To, czy zawiadomienia dokonano bez zbędnej zwłoki, ustala się z uwzględnieniem:

- charakteru i wagi naruszenia ochrony danych osobowych;
- jego konsekwencji; oraz
- niekorzystnych skutków dla osoby, której dane dotyczą.

Zgłoszenie naruszenia ochrony danych osobowych musi co najmniej:

- opisywać 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, których dotyczy naruszenie;
- zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
- opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
- opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Administrator dokumentuje naruszenia ochrony danych osobowych **wg załącznika nr 5**.

Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych to administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

5.OCENA SKUTKÓW DLA OCHRONY DANYCH OSOBOWYCH I UPRZEDNIE KONSULTACJE

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 wg **załącznika nr 1**.

Przy ocenie skutków administrator zasięga opinii inspektora ochrony danych.

Administrator konsultuje z inspektorem ochrony danych następujące kwestie:

- należność przeprowadzenia oceny skutków dla ochrony danych, metodologii przeprowadzenia oceny skutków dla ochrony danych;
- należność przeprowadzenia wewnętrznej oceny lub zlecenia jej podmiotowi zewnętrznemu;
- skuteczność zabezpieczeń (w tym środków technicznych i organizacyjnych) stosowanych do łagodzenia wszelkich zagrożeń praw i interesów osób, których dane dotyczą;
- prawidłowość przeprowadzonej oceny skutków dla ochrony danych i zgodności jej wyników z RODO (czy należy kontynuować przetwarzanie, czy też nie, oraz jakie zabezpieczenia należy zastosować).

W przypadku, gdy administrator nie zgadza się z zaleceniami inspektora ochrony danych w wyżej wymienionych przypadkach, dokumentacja oceny skutków dla ochrony danych osobowych powinna zawierać pisemne uzasadnienie nieuwzględnienia zaleceń.

W sytuacji, gdy zmienia się ryzyko wynikające z operacji przetwarzania, administrator powinien dokonać przeglądu, by stwierdzić, czy przetwarzanie odbywa się zgodnie z oceną skutków dla ochrony danych. Jeżeli ocena ta wykaże, że przetwarzanie może powodować wysokie ryzyko przy braku zastosowania przez administratora środków dla zminimalizowania tego ryzyka, to zgodnie z art. 36 RODO administrator konsultuje się w tej sprawie z organem nadzorczym.

6. WYKAZ ZBIORÓW DANYCH OSOBOWYCH

Dane osobowe wymagające ochrony zostały wykazane wg **załącznika nr 1.**

Każdy ze zbiorów jest opisany w sposób umożliwiający przeprowadzenie analizy ryzyka.

Opis zbiorów obejmuje takie informacje, jak:

- nazwa zbioru i struktura zbioru;
- aktywa służące do przetwarzania danych osobowych (programy i systemy informatyczne, infrastruktura, outsourcing);
- informacja o konieczności przeprowadzenia oceny skutków dla zbioru.

7. PRAWA OSOBY, KTÓREJ DANE DOTYCZĄ

7.1 OBOWIĄZEK INFORMACYJNY

Osoba, której dane dotyczą, jest informowana o **prowadzeniu operacji przetwarzania i o jego celach**. Ponadto administrator podaje wszelkie inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania, uwzględniając konkretne okoliczności i kontekst przetwarzania danych osobowych.

Dodatkowo informuje o fakcie profilowania oraz o konsekwencjach. W przypadku zbierania danych od osoby, której dane dotyczą, wskazuje, czy ma ona obowiązek je podać, oraz o konsekwencjach ich niepodania.

Administrator, w przypadku, gdy zbiera dane osobowe, od osoby której dane dotyczą zgodnie z art. 13 ust. 1 i 2 RODO informuje o:

- swojej tożsamości i danych kontaktowych oraz tożsamość i danych kontaktowych swojego przedstawiciela, jeżeli istnieje;
- danych kontaktowych inspektora ochrony danych;
- celach przetwarzania, do których mają posłużyć dane osobowe;
- podstawie prawnej przetwarzania;
- prawnie uzasadnionym interesie realizowanym przez administratora lub przez stronę trzecią – jeżeli przetwarzanie odbywa się na podstawie prawnie usprawiedliwionego interesu administratora (art. 6 ust. 1 lit. f RODO);
- odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
- transferze danych do państwa trzeciego, w tym o:
  a) zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej;
  b) stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony;
  c) lub wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych w przypadku przekazania danych do państwa trzeciego , o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO;
- okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
- prawie do:

a) żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą ich sprostowania, usunięcia lub ograniczenia przetwarzania lub wniesienia sprzeciwu wobec przetwarzania, a także przenoszenia danych;

b) cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem jeżeli przetwarzanie odbywa się na podstawie zgody na przetwarzanie danych zwykłych (art. 6 ust. 1 lit. a) RODO) lub szczególnej kategorii (art. 9 ust. 2 lit. a RODO);

c) wniesienia skargi do organu nadzorczego;

d) informacji, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;

e) informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotnych informacji o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Wzór obowiązku informacyjnego znajduje się **w załączniku nr 6**.

7.2. PRAWO DOSTĘPU DO DANYCH

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:

- cele przetwarzania;
- kategorie odnośnych danych osobowych;
- informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
- w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
- prawo do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
- prawo wniesienia skargi do organu nadzorczego;
- jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;
- informacje o zautomatyzowane podejmowanie decyzji, w tym profilowanie, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także znaczenie i przewidywane konsekwencje takiego przetwarzania dla osoby, której dane dotyczą.

Wniosek od osoby uprawnionej jest przekazywany administratorowi lub inspektorowi ochrony danych a następnie administrator w porozumieniu z inspektorem ochrony danych dokonuje się potwierdzenia tych danych.

7.3. PRAWO DO SPROSTOWANIA DANYCH

Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia. Sprostowania danych, dokonuje administrator w porozumieniu z inspektorem ochrony danych.

7.4. PRAWO DO USUNIĘCIA DANYCH („PRAWO DO BYCIA ZAPOMNIANYM")

Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, o ile zachodzi jedna z przesłanek wskazana w art. 17 RODO.

Usunięcia danych, dokonuje administrator w porozumieniu z inspektorem ochrony danych.

7.5. PRAWO DO OGRANICZANIA PRZETWARZANIA

Osoba, której dane dotyczą, ma prawo żądania od administratora ograniczenia przetwarzania w następujących przypadkach:

- osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych;
- przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
- administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
- osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

7.6. POWIADOMIENIE O SPROSTOWANIU LUB USUNIĘCIU DANYCH

Administrator informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, których dokonał zgodnie z art. 16, art. 17 ust. 1 i art. 18 RODO, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

Podmiot danych w celu realizacji praw wskazanych w pkt. 7.2-7.6 składa wniosek **wg załącznika nr 7.**

7.7. PRZENOSZENIE DANYCH

Prawo to zapewnia osobom, których dane dotyczą, możliwość otrzymywania w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, danych osobowych, które dostarczyły administratorowi, oraz możliwość przesłania tych danych osobowych innemu administratorowi bez przeszkód.

Podmiot danych składa wniosek **wg załącznika nr 8**.

Zgodnie z treścią art. 20 ust. 1 lit. a) RODO, prawo do przenoszenia danych znajduje zastosowanie wobec operacji przetwarzania danych na podstawie:

a) zgody podmiotu danych;

b) umowy, której podmiot danych jest stroną.

Administrator po konsultacji z inspektorem ochrony danych przekazuje dane za pomocą takich narzędzi jak: „streaming”, płyta CD, DVD lub inny fizyczny nośnik bądź przesyła dane bezpośrednio innemu administratorowi (zgodnie z artykułem 20 ust. 2 RODO, gdy jest to technicznie wykonalne).

8. ZABEZPIECZENIE DANYCH – ŚRODKI TECHNICZNE I ORGANIZACYJNE

8.1. ŚRODKI ORGANIZACYJNE OCHRONY DANYCH OSOBOWYCH

- W celu stworzenia właściwych zabezpieczeń, które powinny bezpośrednio oddziaływać na procesy przetwarzania danych, wprowadza się następujące środki organizacyjne:
  a) przetwarzanie danych osobowych administratora może odbywać się wyłącznie w ramach wykonywania zadań służbowych (zakres uprawnień wynika z zakresu tych zadań);
  b) do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające stosowne upoważnienie nadane przez administratora lub inspektora ochrony danych wg **załącznika nr 9**;
  c) unieważnienie upoważnienia następuje na piśmie, wg wzoru stanowiącego **załącznik nr 10**;
  d) administrator prowadzi ewidencję osób upoważnionych wg **załącznika nr 11** oraz na jej podstawie przygotowuje upoważnienia. Każdy upoważniony do przetwarzania danych potwierdza pisemnie fakt zapoznania się z niniejszą dokumentacją, zrozumieniem wszystkich zasad bezpieczeństwa oraz zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczania. Wzór potwierdzenia stanowi **załącznik nr 12**;
  e) administrator wprowadza **politykę kluczy**. Pomieszczenia biurowe zamykane są na klucz, zabezpieczane są kartą dostępu lub zamkami szyfrowymi. Każdy pracownik odpowiada za swój klucz, kartę lub kod dostępu. W przypadku zagubienia klucza lub karty należy niezwłocznie poinformować o tym fakcie administratora;
- W celu zapobiegania nieautoryzowanemu dostępowi do informacji lub kradzieży informacji i środków jej przetwarzania stosuje się **politykę czystego biurka**. Ważne dokumenty i nośniki zawierające dane osobowe nie powinny pozostać niezabezpieczone w czasie nawet chwilowej nieobecności w pokoju. Pokój należy zamknąć w sposób uniemożliwiający dostęp dla osób nieuprawnionych. Po zakończeniu pracy ważne dokumenty komputerowe i nośniki z danymi osobowymi powinny być przechowywane w szafach, a pokoje powinno się zamykać. Szczególną uwagę należy zwrócić na drukarki sieciowe i kserokopiarki dostępne dla większej liczby pracowników. Pracownicy powinni odbierać dokumenty natychmiast po wykonaniu przez urządzenie zleconego zadania. Nie powinny one pozostawać dostępne ani dla obcych osób ani dla pracowników nieposiadających stosownych uprawnień.

- **Polityka czystego ekranu** ma na celu zabezpieczenie przed nieautoryzowanym dostępem do systemu informatycznego i zabezpieczeniem przed ujawnieniem informacji chronionych. Każdorazowe odejście od stanowiska pracy powinno być poprzedzone wylogowaniem się lub zablokowaniem dostępu do systemu tak, aby niemożliwe było uzyskanie nieautoryzowanego dostępu do systemu. W tym celu każdy komputer ma wprowadzony system automatycznego uruchamiania się wygaszania ekranu i wylogowania użytkownika lub automatycznej blokady dostępu do systemu informatycznego. Po zakończeniu pracy należy zamknąć aktywne aplikacje oraz wyrejestrować się (wylogować się) z systemu lub też zablokować dostęp do systemu.
- Zabrania się udzielania informacji o danych osobowych w formie telefonicznej bez weryfikacji tożsamości rozmówcy.

8.2. ŚRODKI TECHNICZNE OCHRONY DANYCH OSOBOWYCH

Mając świadomość, że żadne zabezpieczenie techniczne nie gwarantuje stuprocentowego bezpieczeństwa danych, konieczne jest, aby każdy użytkownik mający styczność z przetwarzanymi danymi, świadom odpowiedzialności, postępował zgodnie z przyjętymi w niniejszym dokumencie zasadami i minimalizował zagrożenie wynikające z błędów ludzkich. Ochrona danych osobowych przetwarzanych przez administratora obowiązuje wszystkie osoby, które mają dostęp do informacji zbieranych, przetwarzanych oraz przechowywanych, bez względu na zajmowane stanowisko oraz miejsce wykonywania jak również charakter stosunku pracy. Osoby mające dostęp do danych osobowych są zobligowane do stosowania niezbędnych środków zapobiegających ujawnieniu tych danych osobom nieupoważnionym. Przetwarzać dane osobowe w systemach informatycznych jak i tradycyjnych zbiorach papierowych u administratora może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych. Administrator jest odpowiedzialny za opracowanie, wdrożenie i interpretację Polityki Ochrony Danych Osobowych, standardów, zaleceń oraz procedur w całym systemie.

Zbiory danych u administratora zabezpiecza się poprzez:

- Środki ochrony fizycznej:

a) Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi)

b) Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności na włamanie - drzwi klasy C

c) Zbiór danych osobowych przechowywany jest w pomieszczeniu, w którym okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej

d) Pomieszczenia, w którym przetwarzany jest zbiór danych osobowych wyposażone są w system alarmowy przeciwwłamaniowy

e) Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej niemetalowej szafie

f) Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej niemetalowej szafie

g) Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętym sejfie lub kasie pancernej

h) Pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą wolnostojącej gaśnicy

i) Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów

- Środki sprzętowe, infrastruktury informatycznej i telekomunikacyjnej:
  a) Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora (login) użytkownika oraz hasła
  b) Zastosowano systemowe mechanizmy wymuszający okresową zmianę haseł
  c) Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity
  d) Użyto system Firewall do ochrony dostępu do sieci komputerowej

- Środki ochrony w ramach systemowych narzędzi programowych i baz danych:
  a) Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła z wyłączeniem aplikacji biurowych (takich jak produkty Microsoft Office, procesory tekstu, arkusze kalkulacyjne, programy pocztowe)
  b) Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych
  c) Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe

Szczegółowe środki ochrony technicznej systemu informatycznego, jak również wszystkie niezbędne informacje dotyczące jego pracy oraz zasad użytkowania zawarte są w punkcie 15**.**

Administrator dokłada szczególnej staranności w celu zapewnienia, że wszystkie podmioty, którym powierza się przetwarzanie danych osobowych gwarantują środki zabezpieczeń co najmniej na poziomie uznanym przez administratora za obligatoryjny. Administrator dokonuje oceny czy podmiot mający w jego imieniu przetwarzać dane osobowe spełnia wymogi dotyczące środków zabezpieczeń kierując się w szczególności kryteriami wg **załącznika nr 3**.

8.3. MONITOROWANIE I PRZEGLĄD SYSTEMU OCHRONY DANYCH

System Ochrony Danych jest monitorowany poprzez podjęcie następujących działań:

- wykonywanie audytów wewnętrznych przez inspektora ochrony danych;
- wykonywanie okresowych przeglądów dokonywanych przez kierownictwo;
- wykonywanie analizy ryzyka.

8.4. PROCEDURA NADAWANIA UPRAWNIEŃ

Obieg informacji dotyczących nadawania uprawnień przedstawia się następująco:

Osoba odpowiedzialna u administratora za zatrudnienie przygotowuje niezbędne dokumenty i dokonuje niezbędnych czynności w stosunku do każdej nowozatrudnionej osoby mającej przetwarzać dane osobowe, celem nadania jej uprawnień oraz jej przeszkolenia, zgodnie z procedurą wg załącznika nr 13.

W przypadku, gdy nowozatrudniona osoba będzie przetwarzała dane w systemach informatycznych, osoba odpowiedzialna u administratora za zatrudnienie (w razie potrzeby po konsultacji z inspektorem ochrony danych) wnioskuje do administratora celem przydzielenia i zarządzania uprawnieniami w systemie informatycznym. Administrator po nadaniu uprawnień użytkownikowi (identyfikatora i hasła), przekazuje osobie odpowiedzialnej u administratora za zatrudnienie informację o nadaniu uprawnień za pomocą maila.

9. SZKOLENIA OSÓB PRZETWARZAJĄCYCH DANE OSOBOWE

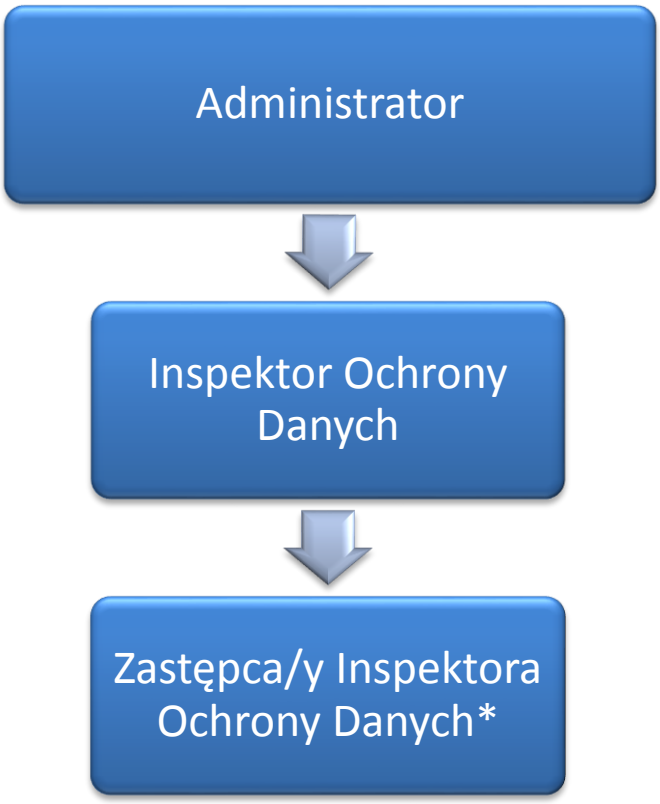
Każda osoba przed dopuszczeniem do pracy z danymi osobowymi powinna zostać przeszkolona i zapoznana z przepisami z zakresu ochrony danych osobowych, w szczególności regulacjami wewnętrznymi zawartymi w Polityce Ochrony Danych Osobowych oraz przepisami RODO. Za przeprowadzenie szkolenia odpowiada inspektor ochrony danych. Potwierdzeniem zapewnienia zapoznania przepisów stanowi pozytywnie zdany test (min. 60% poprawnych odpowiedzi). Szkolenia są przeprowadzane cyklicznie co najmniej raz w roku. Potwierdzenie odbycia szkolenia przez uczestników zawiera w szczególności **załącznik nr 14** lub inny dokument dowodzący faktu przeszkolenia (np. test, certyfikat, wykaz). Po przeszkoleniu z zasad ochrony danych osobowych, uczestnicy zobowiązani są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania.

10. ODPOWIEDZIALNOŚĆ ZA BEZPIECZEŃSTWO INFORMACJI

Odpowiedzialność za bezpieczeństwo informacji ponoszą wszystkie osoby przetwarzając dane osobowe zgodnie z posiadanymi zakresami obowiązków. Każda osoba obowiązana jest dbać o bezpieczeństwo powierzonych mu do przetwarzania, archiwizowania lub przechowywania informacji zgodnie z obowiązującymi przepisami wewnętrznymi w tym m.in.:

- stosować zasady opisane w Polityce Ochrony Danych oraz innych dokumentach wewnętrznych;
- chronić informacje podlegające ochronie przed dostępem do nich osób nieuprawnionych;
- chronić dane przed przypadkowym lub umyślnym zniszczeniem, utratą lub modyfikacją;
- chronić sprzęt, wydruki komputerowe i inne nośniki zawierające dane chronione;
- utrzymywać w tajemnicy powierzone hasła, częstotliwość ich zmiany oraz szczegóły technologiczne systemów także po ustaniu zatrudnienia
- powiadomić administratora lub inspektora ochrony danych o:
  a) ujawnieniu lub możliwości ujawnienia informacji chronionych osobom nieupoważnionym;
  b) nieautoryzowanej zmianie informacji chronionych lub możliwości wprowadzenia nieautoryzowanych zmian;
  c) zniszczeniu lub możliwości zniszczenia informacji chronionych;
  d) zablokowaniu lub możliwości zablokowania pracy systemu informatycznego przetwarzającego informacje chronione lub uniemożliwienia innego dostępu do informacji chronionych.

Na potrzeby Polityki przedstawiono poniższy schemat ról, w którym zdefiniowano role mające szczególne obowiązki w obszarze ochrony danych osobowych.



*Jeżeli wyznaczono

10.1. ADMINISTRATOR

Administrator:

- wprowadza, zarządza i sprawuje nadzór nad działaniami Polityki Ochrony Danych Osobowych;
- określa rodzaje zasobów podlegających ochronie;
- decyduje o celach i środkach przetwarzania danych;
- zatwierdza Politykę Ochrony Danych Osobowych;
- prowadzi komunikację z podmiotem danych i przekazuje mu informacje w sposób zwięzły, przejrzysty, zrozumiały i łatwo dostępny;
- ułatwia podmiotom danych wykonywanie ich praw;
- nieodpłatnie udziela podmiotom danych informacji, również na ich żądanie;
- weryfikuje tożsamość osób wnoszących żądania udzielenia informacji;
- potwierdza czy przetwarzane są dane osobowe dotyczące danej osoby fizycznej, a jeżeli ma to miejsce, udziela wskazanych rozporządzeniem informacji;
- ułatwia osobie, której dane dotyczą wykonywanie jej praw z art. 22 RODO;
- informuje osobę, której dane dotyczą, o działaniach jakie podjął, w związku z jej żądaniami opartymi o art. 22 RODO;
- uzasadnienia odrzucenie żądania osoby, której dane dotyczą i poucza ją o prawie skargi;
- umożliwia dostęp do jej danych osobie, której one dotyczą;
- dokonuje sprostowania i uzupełniane danych;
- usuwa dane;
- powiadamia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu ich przetwarzania;
- dokonuje przenoszenia danych.

10.2. INSPEKTOR OCHRONY DANYCH

Zakres zadań inspektora ochrony danych zawiera art. 39 ust. 1 RODO. Wyliczenie zawarte w tym przepisie nie jest jednak katalogiem zamkniętym, ponieważ jeden z obowiązków inspektora ochrony danych można wywodzić też z art. 38 ust. 4 RODO (pełnienie roli punktu kontaktowego, dla osób, których dane dotyczą).

Wobec powyższego zadania inspektora ochrony danych obejmują:

- informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
- monitorowanie przestrzegania RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków;
- działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
- udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
- współpraca z organem nadzorczym;
- pełnienie funkcji 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 prowadzenie konsultacji we wszelkich innych sprawach;
- pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO;
- prowadzenie rejestru czynności lub rejestru kategorii czynności.

11. AUDYTY

Zgodnie z art. 32 RODO, administrator powinien regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Na podstawie art. 39 ust. 1 RODO inspektor ochrony danych przeprowadza cykliczne audyty.

Celem audytów wewnętrznych jest ocena, czy system ochrony danych osobowych jest skutecznie wdrożony i funkcjonuje zgodnie z wymaganiami RODO. Audyty prowadzone są w sposób obiektywny i bezstronny:

- inspektor ochrony danych jest odpowiedzialny za planowanie i przeprowadzanie audytów wewnętrznych z roczną częstotliwością lub częściej;
- inspektor ochrony danych opracowuje programy audytów wg **załącznika nr 15**, biorąc pod uwagę ważność procesów przetwarzania oraz audytowanych obszarów, jak też wyniki wcześniejszych audytów. Określa on kryteria audytu, jego cel, zakres i ewentualnie metody;
- inspektor ochrony danych jest zobowiązany do przygotowania się do przeprowadzenia audytu, zapoznając się z opisem audytowanego obszaru, stosowanych procedur i wyników poprzednich audytów;
- inspektor ochrony danych realizuje działania audytowe mające na celu uzyskanie obiektywnych dowodów potwierdzających poprawność realizowanych zadań, procedur, polityk, zabezpieczeń, celów, spełniania wymagań RODO;
- w przypadku stwierdzenia uchybień mających wpływ na skuteczność działania systemu ochrony danych zgodnego z RODO, inspektor ochrony danych identyfikuje tzw. uchybienia lub spostrzeżenia;
- wynik audytu zostaje udokumentowany przez inspektora ochrony danych i przekazany administratorowi wg **załącznika nr 16;**
- inspektor ochrony danych dokonuje przeglądu i analizy wyniku audytu oraz decyduje o inicjowaniu działań korygujących, w przypadku zaistnienia poważnych uchybień.

12. PROCEDURA PRZYWRÓCENIA DOSTĘPNOŚCI DANYCH OSOBOWYCH I DOSTĘPU DO NICH W RAZIE INCYDENTU FIZYCZNEGO LUB TECHNICZNEGO. ZARZĄDZANIE CIĄGŁOŚCIĄ DZIAŁANIA

Zgodnie z art. 32 RODO, administrator powinien zapewnić zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

Administrator dba o zapewnienie ciągłości funkcjonowania usług związanych z przetwarzaniem informacji. Celem takiego postępowania jest przeciwdziałanie przerwom w działalności oraz ochrona krytycznych procesów przed rozległymi awariami lub katastrofami.

Powyższe cele realizowane są dzięki:

- podziałowi odpowiedzialności i obowiązków, umożliwiając pracownikom dopilnowanie, wczesne wykrycie i zminimalizowanie zagrożeń mogących mieć wpływ na ciągłość działania;
- wdrożeniu planów ciągłości działania.

O konieczności tworzenia planu ciągłości działania dla konkretnego systemu informatycznego decyduje administrator na podstawie analizy ryzyka.

13. PROCEDURA ANALIZY RYZYKA / OCENA SKUTKÓW

13.1. ZAGADNIENIA OGÓLNE DOTYCZĄCE ANALIZY RYZYKA

Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń.

Celem analizy ryzyka jest zastosowanie środków technicznych i organizacyjnych zapewniających stopień bezpieczeństwa odpowiadający ryzyku wynikającemu z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

W przypadku konieczności przeprowadzenia oceny skutków (art. 35 RODO), wymagane jest wykonanie następujących czynności:

- systematyczny opis planowanych operacji przetwarzania i celów przetwarzania;
- ocena, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
- ocena ryzyka środki planowane w celu zaradzenia ryzyku, przedstawione w postaci planu postępowania z ryzykiem.

13.2. DEFINICJE

- aktywa – środki materialne i niematerialne mające wpływ na przetwarzanie danych osobowych;
- naruszenie (incydent) ochrony danych osobowych – to 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;
- zagrożenie – potencjalne naruszenie (potencjalny incydent);
- skutki – rezultaty niepożądanego incydentu (straty w wypadku wystąpienia zagrożenia);
- ryzyko – prawdopodobieństwo, że określone zagrożenie wystąpi i spowoduje straty lub zniszczenie zasobów.

13.3. POTENCJALNE AKTYWA PODLEGAJĄCE ANALIZIE RYZYKA ORAZ OCENIE SKUTKÓW

- analizie ryzyka poddawane są zbiory danych osobowych, procesy przetwarzania, środki zabezpieczeń, np. zbiór pracowników, zbiór klientów, proces wysyłania informacji handlowej z bazy marketingowej banku, zasady rozliczalności, integralności, poufności, itp.;
- do analizy wymagane jest zidentyfikowanie aktywów;
- wykaz przykładowych aktywów znajduje się w **załączniku nr 17**.

13.4. WYZNACZENIE ZAGROŻEŃ

- administrator, w porozumieniu z inspektorem ochrony danych, jest odpowiedzialny za określenie listy możliwych zagrożeń, które mogą wystąpić w przetwarzaniu danych w zbiorze lub w procesie przetwarzania;
- zagrożenia powinny być identyfikowane w odniesieniu do aktywów (wykaz przykładowych zagrożeń znajduje się w odrębnym dokumencie jakim jest ,,Analiza zagrożeń i ryzyka”).

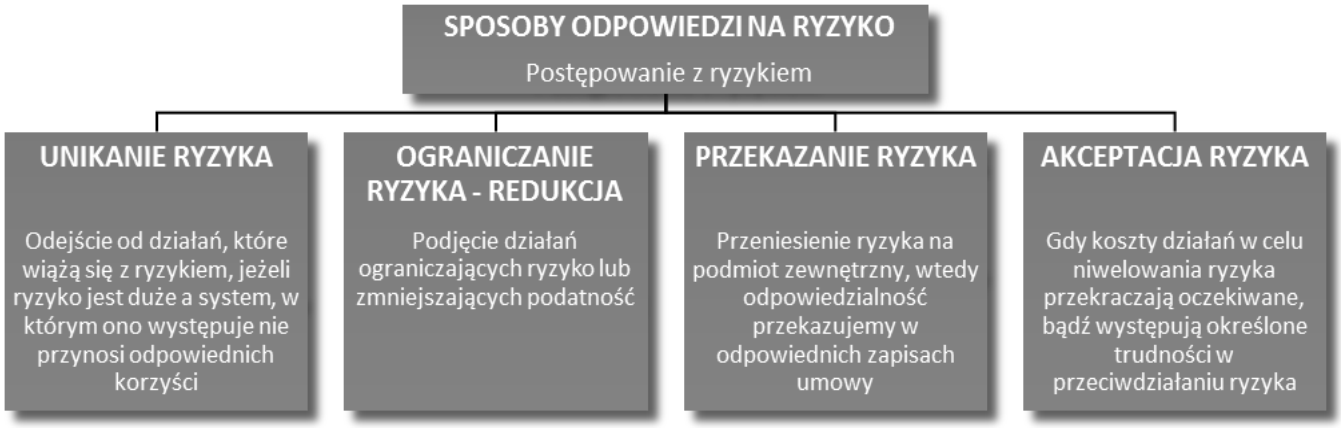
13.5. WYLICZENIE RYZYKA DLA ZAGROŻEŃ

- inspektor ochrony danych określa Prawdopodobieństwo (**P**) wystąpienia poszczególnych zagrożeń w zbiorze lub w procesie przetwarzania (proponowana skala prawdopodobieństwa jest wskazana w dokumencie ,,Analiza zagrożeń i ryzyka")
- inspektor ochrony danych określa przykładowe skutki (**S**) wystąpienia incydentów (materializacji zagrożeń), uwzględniając straty finansowe, utratę reputacji (proponowaną skala skutków znajduje się w dokumencie ,, Analiza zagrożeń i ryzyka")
- inspektor ochrony danych wylicza Ryzyka (**R**) dla wszystkich zagrożeń i ich skutków w/g formuły: **R = P * S**

13.6. PORÓWNANIE WYLICZONYCH RYZYK ZE SKALĄ I OKREŚLENIE DALSZEGO POSTĘPOWANIA Z RYZYKIEM

- inspektor ochrony danych porównuje wyliczone ryzyka ze skalą i podejmuje decyzje dotyczące dalszego postępowania z ryzykiem;

Proponowaną skalę ryzyka prezentuje poniższy wykres:



13.7. REAKCJA NA WARTOŚĆ RYZYKA

- akceptacja ryzyka – zabezpieczenia są właściwe – brak potrzeby stosowania dodatkowych zabezpieczeń;
- działania obniżające ryzyko, które może zastosować administrator:

    a) przekazanie – przerzucenie ryzyka (outsourcing, ubezpieczenie);
    b) unikanie – eliminacja działań powodujących ryzyko (np. zakaz wynoszenia komputerów przenośnych poza obszar organizacji);
    c) redukcja – zastosowanie zabezpieczeń w celu obniżenia ryzyka (np. zaszyfrowanie pendrive'ów z danymi wynoszonych poza firmę).

13.8. PLAN POSTĘPOWANIA Z RYZYKIEM

- wszędzie, gdzie inspektor ochrony danych decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne;
- inspektor ochrony danych zobowiązany jest do monitorowania wdrożenia zabezpieczeń.

13.9. PONOWNA ANALIZA ZAGROŻEŃ I RYZYKA

Ponowna ,,Analiza zagrożeń i ryzyka" przeprowadzana jest cyklicznie lub po znaczących zmianach w przetwarzaniu danych (np. przetwarzanie nowych zbiorów, nowych procesów przetwarzania, zmiany prawne).

W przypadku, gdy analiza ryzyka prowadzona jest w ramach Oceny skutków, wymagana jest do przeprowadzenia przynajmniej raz na 5 lat.

13.10. NARZĘDZIE DO PRZEPROWADZENIA ANALIZY I SZACOWANIA RYZYKA

Analizę ryzyka oraz szacowanie ryzyka przeprowadza się w specjalnym dokumencie ,,Analiza zagrożeń i ryzyka".

14. PRIVACY BY DESIGN & PRIVACY BY DEFAULT

UWZGLĘDNIANIE PRYWATNOŚCI W FAZIE PROJEKTOWANIA (PRIVACY BY DESIGN) ORAZ DOMYŚLNA OCHRONA DANYCH (PRIVACY BY DEFAULT)

Artykuł 25 RODO wprowadza dwie koncepcje: uwzględnianie ochrony danych w fazie projektowania oraz domyślną ochronę danych. Ustawodawca europejski, nadając charakter prawny rozwijanej już wcześniej koncepcji zapewnienia prywatności na etapie projektowania (*privacy by design*), nazwał ją zasadą uwzględnienia ochrony danych w fazie projektowania. Koncepcja ta zakłada, że wymogi dotyczące ochrony danych osobowych i prywatności powinny być uwzględniane już na wstępnych etapach projektowania usług, produktów bądź systemów mających służyć do przetwarzania danych osobowych. Tym samym dla administratora już na etapie projektowania kwestie ochrony danych stają się jednym z najważniejszych elementów.

Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.

Administrator przyjmuje następujące rozwiązania:

- by ocenić jakie środki będą w danym przypadku właściwe należy uwzględniać czynniki takie jak:
  a) stan wiedzy technicznej;
  b) koszt wdrażania;
  c) charakter, zakres, a także kontekst i cele przetwarzania;
  d) ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikającego z przetwarzania.

- środki służące realizacji tego obowiązku mogą polegać m.in. na:
  a) minimalizacji zakresu przetwarzania danych osobowych sprawdzane poprzez cykliczne audyty oraz analizy ryzyka;
  b) jak najszybszej pseudonimizacji;

c) przejrzystości co do funkcji i przetwarzania sprawdzane poprzez cykliczne audyty oraz analizy ryzyka;

d) umożliwieniu osobie, której dane dotyczą, monitorowania przetwarzania danych poprzez prawo do dostępu danych, sprostowania, zmiany czy ograniczania przetwarzania zgodnie z procedurą wskazaną w rozdziale 7;

e) umożliwieniu zmian i udoskonalaniu zabezpieczeń, co jest sprawdzane poprzez cykliczne audyty oraz analizy ryzyka.

15. BEZPIECZEŃSTWO DANYCH OSOBOWYCH W SYSTEMACH INFORMATYCZNYCH

15.1. POSTANOWIENIA OGÓLNE

Za przestrzeganie zapisów dotyczących bezpieczeństwa danych w systemach informatycznych odpowiedzialny jest administrator. Obszar, w którym są przetwarzane dane, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych. Przebywanie osób nieuprawnionych w obszarze, w którym są przetwarzane dane, jest dopuszczalne za zgodą administratora;

- w przypadku, gdy użytkownik przetwarzający dane osobowe korzysta ze sprzętu IT, zobowiązany jest do jego ochrony przed jakimkolwiek zniszczeniem lub uszkodzeniem. Za sprzęt IT rozumie się: komputery stacjonarne, monitory, drukarki, skanery, ksera, laptopy, służbowe tablety i smartfony. Samowolne otwieranie (demontaż) sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) do lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione;
- użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom, pracownikom innych działów) wgląd do danych wyświetlanych na monitorach komputerowych – **tzw. Polityka czystego ekranu.**

15.2. PROCEDURA NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM ORAZ WSKAZANIE OSOBY ODPOWIEDZIALNEJ ZA TE CZYNNOŚCI.

Upoważnienia do przetwarzania danych osobowych nadawane są w związku z wykonywaniem przez upoważnioną osobę obowiązków lub zadań związanych z przetwarzaniem danych osobowych wg **załącznika nr 9**.

Upoważnienia do przetwarzania danych osobowych rejestrowane są w ewidencji osób upoważnionych do przetwarzania danych osobowych wg **załącznika nr 11**.

15.3. STOSOWANE METODY I ŚRODKI UWIERZYTELNIANIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZENIEM I UŻYTKOWANIEM

Środki uwierzytelniania dostępu do systemu informatycznego służącego do przetwarzania danych osobowych to identyfikator użytkownika i hasło dostępu. Każdy identyfikator użytkownika zabezpieczony jest hasłem:

- hasło nie może składać się z żadnych danych personalnych (imienia, nazwiska, adresu zamieszkania użytkownika lub najbliższych osób) lub ich fragmentów;
- hasło musi składać się z co najmniej 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne;
- hasło nie może składać się z identycznych znaków lub ciągu znaków z klawiatury;
- hasło nie może być jednakowe z identyfikatorem użytkownika;
- hasło musi być unikalne, tj. takie, które nie było poprzednio stosowane przez użytkownika.

Jeżeli system nie wymusza zmiany haseł, użytkownik zobowiązany jest do samodzielnej zmiany hasła. Hasła nie powinny być ujawnianie innym osobom. Nie należy zapisywać haseł na kartkach i w notesach, nie naklejać na monitorze komputera, nie trzymać pod klawiaturą lub w szufladzie. Użytkownik jest zobowiązany do utrzymania hasła w tajemnicy, również po utracie jego ważności. W przypadku złamania poufności hasła, użytkownik zobowiązany jest niezwłocznie zmienić hasło i poinformować o tym fakcie inspektora ochrony danych.

Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego służącego do przetwarzania danych osobowych nie powinien być przydzielany innej osobie. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych osobowych, należy niezwłocznie zablokować w systemie informatycznym służącym do przetwarzania danych osobowych oraz unieważnić przypisane mu hasło.

15.4 PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY PRZEZNACZONE DLA UŻYTKOWNIKÓW SYSTEMU INFORMATYCZNEGO SŁUŻĄCEGO DO PRZETWARZANIA DANYCH OSOBOWYCH

Przed rozpoczęciem przetwarzania danych osobowych użytkownik powinien sprawdzić, czy nie ma oznak fizycznego naruszenia zabezpieczeń. W przypadku wystąpienia jakichkolwiek nieprawidłowości, należy powiadomić inspektora ochrony danych.

Przystępując do pracy w systemie informatycznym służącym do przetwarzania danych osobowych, użytkownik jest zobowiązany wprowadzić swój identyfikator oraz hasło dostępu. Zabrania się wykonywania jakichkolwiek operacji w systemie informatycznym służącym do przetwarzania danych osobowych z wykorzystaniem identyfikatora i hasła dostępu innego użytkownika.

W przypadku czasowego opuszczenia stanowiska pracy, użytkownik musi wylogować się z systemu informatycznego służącego do przetwarzania danych osobowych.

Zakończenie pracy w systemie służącym do przetwarzania danych osobowych powinno być poprzedzone sporządzeniem, w miarę potrzeb, kopii zapasowej danych oraz zabezpieczeniem przed nieuprawnionym dostępem dodatkowych nośników danych płyty CD, pendrive i inne, zawierających dane osobowe. Zakończenie pracy w systemie informatycznym służącym do przetwarzania danych osobowych następują poprzez wylogowanie się z tego systemu.

15.5. PROCEDURY TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA

Kopie zapasowe powinny być kontrolowane przez administratora, w porozumieniu z inspektorem ochrony danych, w szczególności pod kątem prawidłowości ich wykonania poprzez częściowe lub całkowite odtworzenie na wydzielonym sprzęcie komputerowym.

Nośniki informatyczne zawierające dane osobowe lub kopie systemów informatycznych służących do przetwarzania danych osobowych są przechowywane w sposób uniemożliwiający ich utratę, uszkodzenie lub dostęp osób nieuprawnionych.

W przypadku likwidacji nośników informatycznych zawierających dane osobowe lub kopie zapasowe systemów informatycznych służących do przetwarzania danych osobowych należy przed ich likwidacją usunąć dane osobowe lub uszkodzić je w sposób uniemożliwiający odczyt danych osobowych.

15.6. SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE ORAZ KOPII ZAPASOWYCH

Nie należy przechowywać zbędnych nośników informacji zawierających dane osobowe oraz kopii zapasowych, a także wydruków i innych dokumentów zawierających dane osobowe. Po upływie okresu ich użyteczności lub przechowywania, dane osobowe powinny zostać skasowane lub zniszczone tak, aby nie było możliwe ich odczytanie.

Elektroniczne nośniki informacji zawierające dane osobowe oraz kopie zapasowe, a także wydruki i inne dokumenty zawierające dane osobowe przechowywane są w zamykanych szafach w sposób zabezpieczający je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem i zniszczeniem.

W przypadku uszkodzenia lub zużycia nośnika informacji zwierających dane osobowe należy go fizycznie zniszczyć tak, aby nie było możliwe odczytanie danych osobowych.

15.7. SPOSÓB ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO SŁUŻĄCEGO DO PRZETWARZANIA DANYCH OSOBOWYCH PRZED DZIAŁALNOŚCIĄ OPROGRAMOWANIA, KTÓREGO CELEM JEST UZYSKANIE NIEUPRAWNIONEGO DOSTĘPU DO SYSTEMU INFORMATYCZNEGO SŁUŻĄCEGO DO PRZETWARZANIA DANYCH OSOBOWYCH

System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:

- działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego:
  a) poprzez zainstalowanie programu antywirusowego;
  b) poprzez zainstalowanie firewall (zapora sieciowa).
- utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej, na przykład poprzez zastosowanie urządzenia chroniącego system informatyczny przed skutkami awarii zasilania typu UPS, generator prądu i/lub wydzieloną sieć elektroenergetyczną.

Każdy zbiór wczytywany do komputera, w tym także wiadomość e-mail, musi być przetestowany programem antywirusowym. Niedopuszczalne jest stosowanie dostępu do sieci Internet bez aktywnej ochrony antywirusowej oraz zabezpieczenia przed dostępem szkodliwego oprogramowania.

Kopie zapasowe:

- przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem w pomieszczeniu zamkniętym;
- usuwa się niezwłocznie po ustaniu ich użyteczności.

15.8. PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH OSOBOWYCH.

Przeglądy i konserwacje sprzętu komputerowego oraz nośników informacji służących do przetwarzania danych osobowych, przeprowadzane są przez administratora.

W przypadku przekazywania do naprawy sprzętu komputerowego z zainstalowanym systemem informatycznym służącym do przetwarzania danych osobowych lub nośnikiem informacji służących do przetwarzania danych osobowych, powinien on zostać pozbawiony danych osobowych przez fizyczne wymontowanie dysku lub skasowanie danych. W innym przypadku musi być zawarta umowa powierzenia danych osobowych.

Przeglądy techniczne wykonywane muszą być nie rzadziej niż raz w roku.

15.9. PROCEDURA W PRZYPADKU WYSTĄPIENIA INCYDENTÓW.

W przypadku stwierdzenia uchybień dotyczących przetwarzania danych każda osoba powinna o tym fakcie niezwłocznie powiadomić inspektora ochrony danych wg **załącznika nr 4**. Następnie administrator, w porozumieniu z inspektorem ochrony danych, wprowadza zabezpieczenia i procedury, które w przyszłości wyeliminują takie zdarzenia.

15.10. KONTROLA STANU ZABEZPIECZEŃ

Inspektor ochrony danych ma prawo do kontroli stanu zabezpieczeń oraz przestrzegania zasad ochrony danych osobowych w dowolnym terminie.

Należy instalować zalecane przez producentów oprogramowania poprawki i uaktualnienia systemu informatycznego służącego do przetwarzania danych osobowych celem wyeliminowania błędów w działaniu lub poprawienia wydajności działania.

15.11. ZASADY KORZYSTANIA Z INTERNETU

- użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą osoby upoważnionej do administrowania infrastrukturą IT (np. informatyk, administrator systemów informatycznych) i tylko w uzasadnionych przypadkach;
- użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu;
- nie należy korzystać ze stron i serwisów internetowych, na których prezentowane są informacje i treści o charakterze przestępczym, hackerskim, pornograficznym lub innym zabronionym przez prawo, z uwagi na ryzyko zainfrkowania systemu operacyjnego szkodliwym oprogramowaniem
- nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł;
- w przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą ”https:”. Dla pewności należy „kliknąć” na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel;
- należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank.

15.12. ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

- przesyłanie danych osobowych z użyciem maila poza organizację może odbywać się tylko przez osoby do tego upoważnione;
- w przypadku przesyłania danych osobowych poza organizację zaleca się wykorzystywanie mechanizmów kryptograficznych (szyfrowanie transmisji, hasłowanie wysyłanych dokumentów lub plików zzipowanych, podpis elektroniczny);
- użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu;
- zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata;
- nie należy otwierać załączników (plików) w mailach nawet od rzekomo znanych nam nadawców bez weryfikacji tegoż nadawcy. Tego typu maile większości przypadków zawierają załączniki ze szkodliwymi programami, które po „kliknięciu" infekują komputer użytkownika oraz często pozostałe komputery w sieci. W wyniku działania takiego szkodliwego oprogramowania może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowanie m przez kryptowirusy;
- bez weryfikacji wiarygodności nadawcy, nie należy „klikać" na hiperlinki w mailach, gdyż mogą to być hiperlinki do stron zainfekowanych lub niebezpiecznych. Użytkownik „klikając" na taki hiperlink bezwiednie infekuje swój komputer oraz często pozostałe komputery w sieci. W wyniku takiej infekcji może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowanie m przez kryptowirusy;
- należy zgłaszać informatykowi przypadki podejrzanych emaili;
- podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW". Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości"!;
- przy korzystaniu z maila, użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego;
- użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.

16. POSTĘPOWANIE W WYPADKU KLĘSKI ŻYWIOŁOWEJ

Klęską żywiołową jest katastrofa spowodowana działaniem sił przyrody takich jak ogień, huragan, woda lub ich przejawami.

W przypadku wystąpienia zagrożenia powodującego konieczność przeprowadzenia ewakuacji osób lub mienia z pomieszczeń, w których przetwarzane są dane osobowe mają zastosowanie przepisy niniejszego rozdziału oraz innych przepisów szczególnych.

Każda osoba, która będzie świadkiem zbliżania się w/w zagrożeń jest obowiązana powiadomić o tym administratora w każdy możliwy sposób. Numer telefonu administratora jest znany pracownikom i współpracownikom. Osoby biorące udział w akcji ratunkowej mają prawo wejść do pomieszczeń, w których przetwarzane są dane osobowe bez innych obowiązków wskazanych w dokumentacji.

W przypadku ogłoszenia alarmu ewakuacyjnego użytkownicy przebywający w pomieszczeniach, w których przetwarzane są dane osobowe obowiązani są do przerwania pracy, a w miarę możliwości przed opuszczeniem tych pomieszczeń do:

- zamknięcia systemu informatycznego;
- zabezpieczenia danych osobowych przetwarzanych tradycyjnie.

W czasie trwania akcji ratunkowej i po jej zakończeniu administrator oraz obecni użytkownicy powinni w miarę możliwości zabezpieczać dane osobowe przed nieuprawnionym do nich dostępem, o ile nie stoi to w sprzeczności z poleceniami wydanymi przez służby ratunkowe.

17. POSTANOWIENIA KOŃCOWE

Polityka Ochrony Danych Osobowych jest dokumentem wewnętrznym i nie może być udostępniania osobom nieupoważnionym w żadnej formie.

Każda osoba przetwarzająca dane osobowe zapoznaje się z treścią Polityki Ochrony Danych Osobowych oraz zobowiązuje się do bezwzględnego stosowania postanowień w niej zawartych przy przetwarzaniu danych osobowych.

18. ZAŁĄCZNIKI

ZAŁĄCZNIK NR 1 WYKAZ ZBIORÓW

Lp.	Nazwa zbioru danych	Struktura zbioru danych	Forma w jakiej dane są przetwarzane (w tym programy i systemy informatyczne)	Infrastruktura	Outsourcing	Ocena skutków

ZAŁĄCZNIK NR 2 WZÓR UMOWY POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH
(zwana dalej: „Umową")

zawarta w ……, dnia .....,
pomiędzy:

……,
w imieniu której/go działa / reprezentowaną/ym przez: ……,
zwaną dalej: **„Zleceniodawcą"** lub **„Administratorem"**,

a

……..,
reprezentowaną/ym przez:
……,
zwaną dalej: **„Zleceniobiorcą"** lub **„Podmiotem przetwarzającym"**,
zwanymi dalej łącznie: „Stronami",

o treści następującej.

§ 1
Powierzenie przetwarzania danych osobowych

W związku z zawarciem pomiędzy Stronami umowy nr …… z dnia ……., której przedmiotem jest ……..(zwanej dalej: **„Umową główną"**), w trakcie której realizacji Zleceniobiorca będzie przetwarzał dane osobowe, o których mowa w § 2 Umowy, Administrator w trybie art. 28 rozporządzenia Parlamentu Europejskiego i Rady Unii Europejskiej 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (zwanego dalej: **„Rozporządzeniem"**) powierza Zleceniobiorcy przetwarzanie tych danych osobowych na zasadach szczegółowo wskazanych w niniejszej Umowie.

§ 2
Kategorie osób, których dotyczy powierzenie przetwarzania danych osobowych oraz rodzaj powierzonych danych osobowych

Powierzenie przetwarzania danych osobowych obejmuje kategorie osób oraz rodzaj dotyczących ich danych osobowych w celu niezbędnym do realizacji przez Zleceniobiorcę Umowy głównej.

§ 3

Cel i charakter przetwarzania danych osobowych

1. Administrator upoważnia Zleceniobiorcę do przetwarzania danych osobowych, o których mowa w Umowie i poleca mu przetwarzanie tych danych osobowych, wyłącznie w celu niezbędnym do realizacji przez Zleceniobiorcę Umowy głównej i wyłącznie w zakresie, jaki jest niezbędny do realizacji tego celu.
2. Przez przetwarzanie danych osobowych rozumie się wszelkie operacje wykonywane na danych osobowych, takie 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.

§ 4

Czas trwania przetwarzania

1. Zleceniobiorca uprawniony jest do przetwarzania powierzonych danych osobowych wyłącznie w okresie obowiązywania Umowy głównej, z zastrzeżeniem § 4 ust. 2 Umowy.
2. Po zakończeniu realizacji Umowy Głównej, Podmiot przetwarzający zobowiązany jest do usunięcia lub zwrotu Administratorowi powierzonych danych osobowych oraz wszelkich ich istniejących kopii, zależnie od wyboru Administratora, chyba że przepisy prawa powszechnie obowiązującego nakazują ich przechowywanie.

§ 5

Oświadczenie Podmiotu przetwarzającego

1. Podmiot przetwarzający oświadcza, że dysponuje środkami technicznymi i organizacyjnymi gwarantującymi przetwarzanie powierzonych danych osobowych zgodnie z Rozporządzeniem oraz niniejszą Umową, w szczególności w sposób chroniący prawa osób, których dane dotyczą oraz że dysponuje środkami technicznymi i organizacyjnymi gwarantującymi przetwarzanie zgodnie z nimi powierzonych danych osobowych.
2. Wymogi wynikające z § 5 ust. 1 Umowy mogą być uznane za zrealizowane przez Podmiot przetwarzający, jeżeli Administrator zaakceptuje przedłożony przez Podmiot przetwarzający:
   a) zatwierdzony kodeks dobrych praktyk w rozumieniu art. 40 Rozporządzenia oraz oświadczenie o spełnianiu wymogów wynikających z tego kodeksu,

b) certyfikat w rozumieniu art. 42 Rozporządzenia wydany przez podmiot certyfikujący, kryteria certyfikacji oraz oświadczenie Podmiotu przetwarzającego o dalszej realizacji kryteriów certyfikacji,
c) dokument dobrych praktyk wydany przez organ nadzorczy, Europejską Radę Ochrony Danych Osobowych lub inny organ nadzorczy w rozumieniu art. 51 Rozporządzenia oraz oświadczenie o spełnieniu wymogów wynikających z dobrych praktyk.

3. Pomimo spełnienia przez Podmiot przetwarzający wymogów, o których mowa w § 5 ust. 2 Umowy, Administrator, uwzględniając kryteria przewidziane w art. 32 ust. 1 RODO, może zażądać od Podmiotu przetwarzającego, przed przystąpieniem przez Podmiot przetwarzający do przetwarzania danych osobowych, przyjęcia i wdrożenia w odpowiednim terminie dodatkowych środków technicznych lub organizacyjnych celem adekwatnego zabezpieczenia powierzonych Podmiotowi przetwarzającemu danych osobowych. W przypadku złożenia takiego żądania przez Administratora, Podmiot przetwarzający nie jest uprawniony do rozpoczęcia przetwarzania danych i w konsekwencji rozpoczęcia realizacji usług, o których mowa w Umowie do momentu realizacji zgłoszonego żądania.

§ 6
Szczegółowe zasady przetwarzania danych osobowych

Podmiot przetwarzający zobowiązuje się:

1) stosować środki techniczne i organizacyjne mające na celu należyte, odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, zabezpieczenie powierzonych do przetwarzania danych osobowych, w szczególności zabezpieczyć je przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów prawa oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, zapewniające adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o którym mowa w art. 32 Rozporządzenia;
2) przetwarzać powierzone dane osobowe wyłącznie na udokumentowane polecenie Administratora – co dotyczy również przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakładają na niego przepisy prawa powszechnie obowiązującego; w takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;
3) nadać upoważnienia do przetwarzania powierzonych danych osobowych zatrudnionym przez niego lub współpracujących z nim na podstawie umów cywilnoprawnych osobom, które będą uczestniczyły w przetwarzaniu powierzonych danych osobowych oraz prowadzić ich ewidencję, a także zapewnić, by osoby te zobowiązały się do zachowania w tajemnicy przetwarzanych danych osobowych,

zarówno w trakcie zatrudnienia lub współpracy z Podmiotem przetwarzającym, jak i po jego ustaniu;

4) pomagać Administratorowi wywiązywać się z obowiązków określonych w art. 32-36 Rozporządzenia;
5) w przypadku stwierdzenia naruszenia zasad ochrony i przetwarzania powierzonych danych osobowych, zgłosić je niezwłocznie - najpóźniej jednak w ciągu 24 godzin od stwierdzenia naruszenia – Administratorowi, na adres mailowy przewidziany do komunikacji między Stronami w związku z realizowaniem Umowy głównej;
6) pomagać Administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania przez nią jej praw określonych w Rozporządzeniu.

§ 7
Prawo kontroli

1. Administratorowi lub upoważnionemu przez niego audytorowi zewnętrznemu przysługuje prawo kontroli przestrzegania zasad przetwarzania powierzonych danych osobowych, w szczególności w zakresie przestrzegania postanowień niniejszej Umowy oraz spełnienia wymogów przewidzianych w Rozporządzeniu oraz innych powszechnie obowiązujących przepisach prawa.
2. Podmiot przetwarzający zobowiązany jest na każdy pisemny wniosek Administratora, udzielić w terminie 7 dni od dnia otrzymania takiego wniosku, pisemnej informacji dotyczącej przetwarzania powierzonych mu danych osobowych.
3. Administrator upoważniony jest do realizowania bezpośredniej kontroli przetwarzania powierzonych danych osobowych, w miejscu ich przetwarzania przez Podmiot przetwarzający, po zgłoszeniu takiego zamiaru z minimum 7-dniowym wyprzedzeniem.
4. W przypadku stwierdzenia przez Administratora naruszeń w przetwarzaniu powierzonych danych osobowych, Podmiot przetwarzający zobowiązany jest do ich usunięcia najpóźniej w terminie 7 dni od dnia zgłoszenia takiego żądania przez Administratora i zgodnie z jego zaleceniami.
5. Podmiot przetwarzający zobowiązany jest udostępniać Administratorowi wszelkie informacje niezbędne do wykazania spełnienia przez niego obowiązków określonych w art. 28 Rozporządzenia, a także przyczyniać się do wykonywania przez Administratora przysługującego mu prawa kontroli.
6. Podmiot przetwarzający zobowiązany jest niezwłocznie informować Administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie Rozporządzenia lub innych przepisów prawa powszechnie obowiązujących dotyczących ochrony danych osobowych.

§ 8
Dalsze powierzenie przetwarzania danych osobowych

1. Podmiot przetwarzający może powierzyć dane osobowe powierzone mu do przetwarzania na podstawie niniejszej Umowy do dalszego przetwarzania podmiotom będącym jego podwykonawcami, jedynie w celu realizacji Umowy głównej i wyłącznie po uzyskaniu każdorazowo uprzedniej zgody Administratora, wyrażonej w formie pisemnej pod rygorem nieważności.
2. Podmiot przetwarzający zobowiązany jest nałożyć na podmiot, o którym mowa w § 8 ust. 1 Umowy, takie same obowiązki z zakresu ochrony powierzonych danych osobowych, jakie wynikają z niniejszej Umowy, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie powierzonych danych osobowych odpowiadało wymogom Rozporządzenia oraz innym powszechnie obowiązującym przepisom prawa.
3. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za wszelkie naruszenia obowiązków z zakresu ochrony powierzonych danych osobowych przez podmioty, o których mowa w § 8 ust. 1 Umowy.

§ 9
Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający ponosi odpowiedzialność za udostępnienie lub wykorzystanie powierzonych danych osobowych niezgodnie z postanowieniami Umowy, a w szczególności za udostępnienie tych danych osobowych osobom nieupoważnionym.
2. Podmiot przetwarzający zobowiązany jest niezwłocznie poinformować Administratora o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający powierzonych danych osobowych, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych osobowych, a także o wszelkich planowanych lub realizowanych kontrolach i inspekcjach dotyczących ochrony danych osobowych.

§ 10
Klauzula poufności

1. Podmiot przetwarzający zobowiązuje się względem Administratora do zachowania poufności i nie ujawniania osobom trzecim jakichkolwiek informacji, danych osobowych, dokumentów lub materiałów uzyskanych w związku z wykonywaniem Umowy lub Umowy Głównej (zwanych dalej „Informacjami poufnymi”), chyba że Administrator wyrazi na to zgodę w formie pisemnej pod rygorem nieważności lub że konieczność taka wynika z przepisów prawa powszechnie obowiązującego.
2. Informacje poufne będą wykorzystywane przez Podmiot przetwarzający wyłącznie w celu i w zakresie niezbędnym do realizowania Umowy oraz Umowy głównej.

§ 11
Postanowienia końcowe

1. Wszelkie zmiany, uzupełnienia, rozwiązanie lub wypowiedzenie Umowy powinny być dokonane w formie pisemnej pod rygorem nieważności.
2. W zakresie nieuregulowanym Umową zastosowanie mają przepisy Rozporządzenia, Kodeksu cywilnego oraz inne przepisy prawa powszechnie obowiązującego w Polsce.
3. W przypadku, gdy Umowa odwołuje się do przepisów prawa powszechnie obowiązującego, oznacza to również inne przepisy dotyczące ochrony danych osobowych, a także wszelkie nowelizacje, jakie wejdą w życie po dniu zawarcia Umowy, jak również akty prawne, które zastąpią wskazane ustawy i rozporządzenia.
4. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

…….. ……

Administrator Podmiot przetwarzający

ZAŁĄCZNIK NR 3 JAK POWIERZYĆ PRZETWARZANIE DANYCH OSOBOWYCH W SPOSÓB ZGODNY Z RODO?

I. Wybierz odpowiedni podmiot przetwarzający

Powierzając podmiotowi przetwarzającemu czynności przetwarzania, korzystaj wyłącznie z usług takich podmiotów, które:

- dysponują odpowiednią wiedzą fachową,
- są wiarygodne,
- posiadają odpowiednie zasoby do realizacji przetwarzania powierzonych danych,
- gwarantują, że wdrożyły środki techniczne i organizacyjne odpowiadające wymogom RODO, w tym wymogom bezpieczeństwa przetwarzania oraz wymogom określonym przez administratora.

Możesz skorzystać z podmiotu przetwarzającego, który uzyskał odpowiedni certyfikat wydany na podstawie ogólnego rozporządzenia o ochronie danych.

II. Podpisz umowę powierzenia lub ureguluj powierzenie przy pomocy innych środków zgodnych z RODO

Powierzenie przetwarzania danych osobowych musisz uregulować umową lub innym instrumentem prawnym, określ w nim:

- przedmiot i czas trwania przetwarzania,
- charakter i cele przetwarzania,
- rodzaj danych osobowych,
- kategorie osób, których dane dotyczą,
- konkretne zadania i obowiązki podmiotu przetwarzającego w kontekście planowanego przetwarzania.

Podpisując umowę powierzenia, uwzględnij ryzyko naruszenia praw lub wolności osoby, której dane dotyczą.

III. Uzyskaj potwierdzenie, że podmiot przetwarzający dane spełnia wymogi, jakie nakłada na niego ogólne rozporządzenie o ochronie danych

Podmiot przetwarzający powinien:

- wdrożyć środki techniczne i organizacyjne odpowiednie do ryzyka przetwarzania danych osobowych – tak, by przetwarzanie odpowiadało wymogom ogólnego rozporządzenia o ochronie danych,

- prowadzić rejestr kategorii czynności przetwarzania wykonywanych w imieniu administratora,
- zgłaszać naruszenia ochrony danych do administratora,
- wyznaczyć inspektora ochrony danych (jeśli zobowiązują go do tego przepisy ogólnego rozporządzenia o ochronie danych).

IV. Dokonaj przeglądu podpisanych umów powierzenia

Upewnij się, że podmiot, któremu powierzyłeś przetwarzanie danych osobowych, spełnia wszystkie wymagania zawarte w RODO.
Sprawdź, czy podpisane przez Ciebie umowy powierzenia zawierają wszystkie niezbędne elementy, które wskazuje ogólne rozporządzenie o ochronie danych.

ZAŁĄCZNIK NR 4 RAPORT Z NARUSZENIA BEZPIECZEŃSTWA ZASAD OCHRONY DANYCH OSOBOWYCH

w ……

1. Data: …… Godzina: ……

(dd.mm.rr) *(gg:mm)*

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

……
……..

(imię, nazwisko, stanowisko służbowe)

3. Lokalizacja zdarzenia:

……
……..

(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

……
……

5. Przyczyny wystąpienia zdarzenia:

……
……
……..

6. Podjęte działania:

……
……

7. Środki zaradcze:

……
……

……

Data, miejsce i podpis administratora

ZAŁĄCZNIK NR 5 EWIDENCJA NARUSZEŃ OCHRONY DANYCH OSOBOWYCH

EWIDENCJA NARUSZEŃ OCHRONY DANYCH OSOBOWYCH

(ZGODNIE Z ART. 33 UST.5 RODO)

Lp.	Opis okoliczności naruszenia/ incydentu	Ilość osób dotknięta naruszeniem/ incydentem	Skutki naruszenia/ incydentu	Działania zaradcze	Naruszenie/incydent, skutkujące/ący ryzykiem naruszenia praw lub wolności osób fizycznych. Zgłoszenie Prezesowi Urzędu Ochrony Danych Osobowych (**TAK, NIE**)	Data zakończenia wdrażania działań naprawczych	Osoba odpowiedzialna za wdrożenie działań	Naruszenie ochrony danych osobowych, powodujące wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Zawiadomienie osoby, której dane dotyczą o incydencie (**TAK, NIE**)
1.								
2.								
3.								
4.								
5.								
6.								
7.								

.....

Data, miejsce i podpis administratora

ZAŁĄCZNIK NR 6 WZÓR OBOWIĄZKU INFORMACYJNEGO

(przykład dotyczący pracownika)

OBOWIĄZEK INFORMACYJNY – PRACOWNIK

1. Administratorem Pani/Pana danych osobowych jest:

_____

(pieczątka Administratora)

zwany dalej **Administratorem.** Administrator prowadzi operacje przetwarzania Pani/Pana danych osobowych.
2. Dane kontaktowe Inspektora Ochrony Danych Osobowych (po jego wyznaczeniu): e-mail: inspektor@rodo-krp.pl,
tel. +48 792 304 042.
3. Pani/Pana dane osobowe przetwarzane będą w celu zatrudnienia, szkoleń, podnoszenia kwalifikacji, wypełnienia obowiązków i wykonywania szczególnych praw przez Administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, w celach informacyjnych oraz promocji i budowy wizerunku Administratora.
4. Podstawą przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. a, b, c i art. 9 ust. 2 a, b, h 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) z dnia 27 kwietnia 2016 r. (Dz.Urz.UE.L Nr 119, str. 1, dalej: RODO) oraz inne akty prawne, w szczególności ustawa z dnia 26 czerwca 1974 r. – Kodeks pracy wraz z aktami wykonawczymi, ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej wraz z aktami wykonawczymi, ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny wraz z aktami wykonawczymi, ustawa z dnia 24 kwietnia 2003 r. o działalności pożytku publicznego i o wolontariacie wraz z aktami wykonawczymi, ustawa z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych wraz z aktami wykonawczymi, ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych wraz z aktami wykonawczymi, ustawa z dnia 4 marca 1994 r. o zakładowym funduszu świadczeń socjalnych, ustawa z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych wraz z aktami wykonawczymi.
5. Pani/Pana dane osobowe mogą być przetwarzane również przez podmioty, z którymi Administrator zawarł umowy powierzenia przetwarzania danych osobowych, w szczególności w zakresie obsługi informatycznej, prawnej, kadrowej, księgowej, BHP,

ochrony osób i mienia lub ochrony danych osobowych, a także przez podmioty, którym Administrator udostępnia dane osobowe na podstawie przepisów prawa, w szczególności organom ścigania, organom kontrolnym, organom podatkowym, organom systemu ubezpieczeń społecznych i Narodowemu Funduszowi Zdrowia.

6. Podanie przez Panią/Pana danych osobowych jest niezbędne do zawarcia umowy i wynika z przepisów prawa; w przypadku niepodania tych danych, zawarcie umowy jest niemożliwe. W pozostałym zakresie Pani/Pana dane osobowe mogą być przetwarzane na podstawie udzielonej przez Panią/Pana zgody lub na podstawie innych przesłanek dopuszczalności przetwarzania wskazanych w art. 6 i 9 RODO.
7. Posiada Pani/Pan prawo do:
   a. żądania od Administratora dostępu do swoich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych oraz powiadomienia odbiorców danych o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania;
   b. wniesienia sprzeciwu wobec przetwarzania;
   c. wniesienia sprzeciwu wobec zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach, w tym profilowania;
   d. przenoszenia danych osobowych;
   e. otrzymywania kopii danych osobowych podlegających przetwarzaniu;
   f. wniesienia skargi do organu nadzorczego (obecnie Generalnego Inspektora Ochrony Danych Osobowych, w przyszłości – właściwego w świetle obowiązujących przepisów organu nadzorczego);
   g. cofnięcia zgody na przetwarzanie danych osobowych.
8. Pani/Pana dane osobowe nie podlegają zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.
9. W przypadku wyczerpania przesłanek zawartych w przepisach art. 6 ust. 1 lit. a i art. 9 ust. 2 lit. a RODO, przysługuje Pani/Panu prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.
10. Pani/Pana dane osobowe będą przechowywane przez czas trwania umowy oraz przez wymagany
    w świetle obowiązującego prawa okres po jej wygaśnięciu, w celu archiwizowania danych lub dochodzenia roszczeń.

_____

(data i podpis Administratora)

ZAŁĄCZNIK NR 7 WZÓR WNIOSKU O REALIZACJĘ ŻĄDAŃ PODMIOTU DANYCH

I. Żądanie

1. Data zgłoszenia żądania:

……..

2. Forma zgłoszenia żądania (kanał komunikacji):

……..

3. Zgłaszający żądanie:

……..

4. Treść żądania:

……..

II. Obsługa żądania

1. Pracownik obsługujący żądanie:

……..

2. Czy dane zgłaszającego żądanie są przetwarzane przez administratora danych:

……..

3. Czy dane zgłaszającego żądanie zostały powierzone (komu, kiedy):

……..

4. Podjęte czynności:

a) Czynność I

- Osoba podejmująca czynność:

……..

- Opis czynności:

……..

- Data dokonania czynności:

……..

b) Czynność II

- Osoba podejmująca czynność:

……..

- Opis czynności:

……..

- Data dokonania czynności:

……..

……

podpis wnioskodawcy

ZAŁĄCZNIK NR 8 WNIOSEK O PRZENIESIENIE DANYCH

dn. ……..

……..

(imię i nazwisko wnioskodawcy)

……..

(dane identyfikujące wnioskodawcę)

W N I O S E K

o przeniesienie danych

Na podstawie art. 20 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) wnoszę o przeniesienie danych:

……

……

……

(zakres danych, wskazanie administratora - dotyczy tylko przenoszenia danych do innego podmiotu)

za pomocą:

……

(narzędzia do przenoszenia danych np. płyta CD, DVD, pendrive itp.)

……

podpis wnioskodawcy

ZAŁĄCZNIK NR 9 UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

_____, dnia _____ 2018 roku

UPOWAŻNIENIE I POLECENIE przetwarzania danych osobowych
u Administratora:

_____
(pieczęć Administratora)

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)

upoważniam Panią/Pana* _____
(imię i nazwisko)

do przetwarzania danych osobowych w zakresie i celu niezbędnym do prawidłowego wykonywania u Administratora praw i obowiązków na zajmowanym przez Panią/Pana stanowisku, zgodnie z zakresem kompetencji oraz obowiązków zawodowych i służbowych na tym stanowisku, a także zgodnie z wytycznymi Administratora oraz **polecam Pani/Panu przetwarzanie danych osobowych** w powyższym zakresie i celu. Powyższe upoważnienie i polecenie obejmuje powierzone do przetwarzania dane osobowe przez innego administratora, w zakresie i celu określonym w umowie powierzenia, w przypadku jej zawarcia.

Upoważnienie i polecenie wygasa z chwilą ustania Pana/Pani zatrudnienia lub współpracy (bez względu na podstawę prawną zatrudnienia lub współpracy) lub odwołania upoważnienia. Jednocześnie informuję, że zobowiązany(a) jest Pan(i) do zachowania w tajemnicy powyższych informacji, w szczególności w zakresie danych osobowych i sposobów ich zabezpieczania, również po odwołaniu upoważnienia, a także po ustaniu zatrudnienia lub współpracy.

_____
(podpis Administratora)

ZAŁĄCZNIK NR 10 WZÓR UNIEWAŻNIENIA UPOWAŻNIENIA 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) unieważniam upoważnienie do przetwarzania danych osobowych wydane:

……
……..

(imię i nazwisko, stanowisko)

……..

Data, miejsce i podpis administratora lub inspektora ochrony danych

ZAŁĄCZNIK NR 11 EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Lp.	Nazwisko, Imię	Okres upoważnienia		Uwagi
		OD	DO	
1.			Odwołania/Wygaśnięcia	
2.			Odwołania/Wygaśnięcia	
3.			Odwołania/Wygaśnięcia	
4.			Odwołania/Wygaśnięcia	
5.			Odwołania/Wygaśnięcia	
6.			Odwołania/Wygaśnięcia	
7.			Odwołania/Wygaśnięcia	
8.			Odwołania/Wygaśnięcia	
9.			Odwołania/Wygaśnięcia	
10			Odwołania/Wygaśnięcia	
11.			Odwołania/Wygaśnięcia	
12.			Odwołania/Wygaśnięcia	
13.			Odwołania/Wygaśnięcia	
14			Odwołania/Wygaśnięcia	

…….

data, miejsce i podpis administratora

ZAŁĄCZNIK NR 12 OŚWIADCZENIE O POUFNOŚCI

_____, dnia _____ 2018 roku

_____

(pieczęć Administratora)

_____

(imię i nazwisko)

OŚWIADCZENIE O POUFNOŚCI

Oświadczam, iż zapoznałem/am się z przepisami dotyczącymi ochrony danych osobowych, w szczególności z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) i z regulacjami wewnętrznymi obowiązującymi u Administratora oraz zobowiązuję się do ich stosowania. Jestem świadomy/a obowiązku zachowania w tajemnicy przetwarzanych danych osobowych i sposobów ich zabezpieczania, również po odwołaniu upoważnienia, a także po ustaniu zatrudnienia lub współpracy.

_____

(podpis pracownika/współpracownika)

ZAŁĄCZNIK NR 13 PROCEDURA DOPUSZCZANIA NOWEJ OSOBY DO PRACY/WSPÓŁPRACY U ADMINISTRATORA

Pieczęć administratora

PROCEDURA DOPUSZCZANIA NOWEJ OSOBY DO PRACY/WSPÓŁPRACY U ADMINISTRATORA

1. Niniejsza procedura dotyczy przyjmowania do pracy/współpracy u administratora nowej osoby fizycznej, bez względu na podstawę prawną zatrudnienia/współpracy (umowa o pracę, umowa cywilnoprawna z osobą prowadzącą działalność gospodarcza lub nieprowadzącą działalności gospodarczej).
2. Przed dopuszczeniem do pracy/współpracy:
   a) dana osoba musi zostać przeszkolona w zakresie przepisów prawnych oraz wprowadzonych u administratora zasad dotyczących ochrony danych osobowych (w szczególności z Polityką Ochrony Danych), co musi zostać potwierdzone zdanym przez nią testem. Szkolenie i test może zostać przeprowadzone osobiście lub przy wykorzystaniu informatycznej platformy szkoleniowej (e-learning);
   b) danej osobie administrator musi nadać upoważnienie i wydać polecenie w zakresie przetwarzania danych osobowych, zgodnie ze wzorem stanowiącym załącznik nr 9 do Polityki Ochrony Danych. Oryginał upoważnienia i polecenia zostaje u administratora. Upoważnienie i polecenie należy, na prośbę danej osoby, okazać jej lub wydać jej w kopii. Nadanie nowego upoważnienia należy odnotować w ewidencji upoważnień (załącznik nr 11 do Polityki Ochrony Danych);
   c) dana osoba musi podpisać oświadczenie o zachowaniu poufności, zgodnie ze wzorem stanowiącym załącznik nr 12 do Polityki Ochrony Danych. Oryginał upoważnienia i polecenia zostaje u administratora. Oświadczenie należy, na prośbę danej osoby, wydać jej w kopii;
   d) danej osobie administrator musi wręczyć oryginał podpisanego przez administratora dokumentu realizującego obowiązek informacyjny względem, odpowiednio, osób zatrudnionych na umowach o pracę lub osób współpracujących na umowach (załącznik A lub B do niniejszej procedury). Fakt odbioru ww. dokumentu dana osoba dokumentuje wpisując na kopii ww. podpisanego przez siebie oświadczenia: „Odebrałem oryginał niniejszego dokumentu” i opatrując ten tekst datą i podpisem. Tak podpisana kopia zostaje u administratora;

e) dana osoba musi podpisać zgodę na przetwarzanie danych osobowych, według wzoru stanowiącego załącznik C do niniejszej procedury. W celu zapewnienia sprawnego dalszego funkcjonowania placówki celowe jest zapewnienie, że zaznaczone zostaną przez osoby podpisujące te zgody wszystkie wskazane typy zgód, zgoda musi mieć charakter w pełni dobrowolny. Oryginał dokumentu zgody zostaje u administratora. Dokument zgody należy, na prośbę danej osoby, wydać jej w kopii

3. Powyższe czynności dokonywane są przez dział kadr lub osobę prowadzącą sprawy kadrowe u administratora. Jednak w przypadku jakichkolwiek pytań lub wątpliwości należy skontaktować się z Inspektorem Ochrony Danych.

Zatwierdzam i nakazuję stosować.

_____

data i podpis administratora

ZAŁĄCZNIK NR 14 LISTA UCZESTNIKÓW SZKOLENIA Z ZAKRESU OCHRONY DANYCH OSOBOWYCH

Prowadzący:

Miejsce i data szkolenia:

Lp.	Imię	Nazwisko	Podpis
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			

ZAŁĄCZNIK NR 15 PRZYKŁADOWY PLAN AUDYTU

PRZYKŁADOWY PLAN AUDYTU Z ZAKRESU PRZESTRZEGANIA ZASAD OCHRONY DANYCH OSOBOWYCH

NA OKRES OD 25.05.2018R. DO 31.12.2018R.

Lp.	Przedmiot audytu	Zakres audytu	Data rozpoczęcia	Data zakończenia	Obszar kontroli
1.	Realizacja procedur wdrożonych przez ADO w zakresie ochrony danych osobowych	❖ Ustawienie sprzętu komputerowego w pomieszczeniach – czy uniemożliwia dostęp do ekranu monitorów osobom postronnym ❖ Polityka czystego biurka ❖ Polityka kluczy ❖ Sprawdzenie czy osoby dopuszczone do przetwarzania danych osobowych otrzymały pisemne upoważnienia oraz oświadczenia o zapoznaniu z przepisami oraz wewnętrznymi dokumentami z zakresu ochrony danych osobowych osób dopuszczonych do przetwarzania danych osobowych. ❖ Ustalamy, czy osoby, które nie powinny mieć już prawa dostępu do danych osobowych (np. byli pracownicy) mają odwołane upoważnienia ❖ Ewidencja wydanych upoważnień oraz jej zgodność z wydanymi upoważnieniami	00-00-2018 r.	00-00-2018 r.	
2.	Funkcjonowanie zastosowanych zabezpieczeń	❖ Spełnienie wymogów z poziomu ochrony systemów	00-00-2018 r.	00-00-2018r.	

	fizycznych oraz funkcjonowanie zabezpieczeń systemowych (przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy)	informatycznych służących do przetwarzania danych osobowych przed osobami trzecimi. ❖ Sprawdzenie mechanizmów automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika. ❖ Sprawdzenie czy zbiór danych osobowych formie papierowej przechowywany jest zamkniętej niemetalowej szafie. ❖ Sprawdzenie czy zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi). ❖ Przestrzeganie zasady rozpoczęcia i zakończenia pracy w systemie. ❖ Zabezpieczenie systemowe i fizyczne sprzętu komputerowego. ❖ Tworzenie kopii zapasowych. ❖ Odnotowywanie przez systemy służące do przetwarzania danych osobowych czynności wykonywane na danych osobowych przez użytkowników.			
3.	Prawidłowość	❖ Dostęp pracowników do zbiorów danych oraz	00-00-2018 r.	00-00-2018 r.	

	funkcjonowania mechanizmów kontroli dostępu do zbiorów danych	zakres dostępu pracowników i weryfikacja wydanych upoważnień (w tym byłych pracowników oraz odwołanie upoważnień). ❖ Zasady nadawania/ zmieniania/odbierania uprawnień do systemów informatycznych. ❖ Stosowanie identyfikatorów i haseł dla użytkowników zgodnie z wymogami formalnymi.			
4.	Inwentaryzacja dokumentacji opisującej sposób przetwarzania danych osobowych	❖ Zgodności dokumentacji przetwarzania danych z obowiązującymi przepisami prawa	00-00-2018 r.	00-00-2018 r.	

Dokumentowanie czynności w toku audytu polega w szczególności na:

1. sporządzeniu notatki z czynności, między innymi 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 osoby;
3. sporządzeniu kopii otrzymanego dokumentu, sporządzeniu kopii obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych.

ZAŁĄCZNIK NR 16 SPRAWOZDANIE Z AUDYTU

SPRAWOZDANIE Z AUDYTU

1) Oznaczenie administratora i adres jego siedziby:

……

(pełna nazwa oraz adres)

2) Imię i nazwisko inspektora ochrony danych:

…….

3) Wykaz czynności podjętych przez inspektora ochrony danych w toku audytu oraz imiona, nazwiska i stanowiska osób biorących udział w tych czynnościach:

……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……

4) Data rozpoczęcia i zakończenia audytu:

……

5) Określenie przedmiotu i zakres audytu:

……

6) Opis stanu faktycznego stwierdzonego w toku audytu oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych:

……
……
……
……
……
……
……

7) Stwierdzone przypadki naruszania przepisów o ochronie danych osobowych w zakresie objętym audytem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem:

……
……
……
……
……

8) Wyszczególnienie załączników stanowiących składową część sprawozdania:

……
……
……

……..

Data, miejsce i podpis inspektora ochrony danych

ZAŁĄCZNIK NR 17 AKTYWA ORAZ PODAKTYWA W ZAKRESIE ANALIZ RYZYKA

AKTYWA	PODAKTYWA
1. Informacje	**INFORMACJE**
	dane osobowe
	dane dostępowe (loginy, hasła, piny)
	dane dotyczące zabezpieczeń (klucze szyfrujące, certyfikaty)
	logi systemowe
	dokumentacja techniczna
	polityki bezpieczeństwa
	procedury odtworzeniowe
	umowy
2. Programy i systemy informatyczne	**OPROGRAMOWANIE**
	systemy operacyjne
	oprogramowanie użytkowe (pakiety biurowe, oprogramowanie biznesowe)
	serwery usługowe (www, poczta, serwery plików, bazy danych, usługi katalogowe)
	oprogramowanie administracyjne (wirtualizacja, inwentaryzacja, monitoring, backup)
	sterowniki
	oprogramowanie antywirusowe
	oprogramowanie układowe (firmware)
	oprogramowanie rozwijane we własnym zakresie
	strony www i aplikacje webowe
3. Infrastruktura IT	**SPRZĘT KOMPUTEROWY**
	serwery (fizyczne i wirtualne)
	storage (macierze, NAS-y)
	stacje robocze (PC, laptopy, terminale)
	urządzenia mobilne (tablety, smartfony, terminale)
	urządzenia peryferyjne (drukarki, skanery)

	TELEKOMUNIKACJA
	centrale telefoniczne
	centrale voip
	urządzenia klienckie (telefony, faxy, modemy)
	łącza (Internet, SIP trunki, tunele vpn, linie dedykowane)
	NOŚNIKI DANYCH
	elektroniczne nośniki z danymi
	dokumentacja papierowa
	nośniki instalacyjne
	nośniki licencji
	SIEĆ
	usługi sieciowe (DNS, DHCP, VPN, protokoły routingu)
	okablowanie
	urządzenia aktywne (switche, routery, AP, mediakonwertery)
	urządzenia pasywne (krosownice, patchpanele)
	systemy sieciowe (firewalle, bramki, UTMy, IPSy, IDSy, proxy)
4. Infrastruktura	**OBSZARY CHRONIONE**
	serwerownie
	punkty dystrybucyjne sieci
	punkty składowania i przetwarzania danych (elektronicznych i papierowych)
	studzienki i kanały telekomunikacyjne
	rozdzielnie elektryczne
	stanowiska monitoringu
	SPRZĘT WSPOMAGAJĄCY
	klimatyzatory
	zasilacze awaryjne i agregaty
	monitoring środowiskowy (czujki temp., zalania, dymu)
	systemy automatycznego gaszenia

	monitoring wizyjny (kamery, rejestratory)
	systemy alarmowe
	systemy kontroli dostępu
	rejestratory czasu pracy
5. Pracownicy i współpracownicy	**PERSONEL**
	kompetencje
	doświadczenie
	know-how
6.Outsorcing	**DOSTAWCY**
	oprogramowania
	usług chmurowych
	usług internetowych (hosting, dns, poczta)
	łączy
	usług serwisowych i gwarancyjnych
	wsparcia technicznego

19. ARKUSZ ZMIAN

Lp.	Treść zmiany	Data
1.		
2.		
3.		
4.		
5.		

Lp.	Treść zmiany	Data
1.		
2.		
3.		
4.		
5.		

Lp.	Treść zmiany	Data
1.		
2.		
3.		
4.		
5.		