BezDebetu.pl
Twoja przyjazna księgowość

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

BEZDEBETU.PL SP. Z O. O. SP.K.

WERSJA 2.0

CZERWIEC – 2018 R

SPIS ZAWARTOŚCI:

HISTORIA ZMIAN W DOKUMENCIE

Numer wersji	Data zmiany	Zmiany wprowadził(a)	Opis zmian
1.0	czerwiec 2018 r.	Agata Iwaszko	Opublikowanie wersji 2.0

1. POSTANOWIENIA OGÓLNE

Polityka Bezpieczeństwa Danych Osobowych dla BezDebetu.pl Sp. z o. o. Sp.k. (w dalszej części zwanej również Spółką) jest zbiorem praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji danych osobowych wewnątrz organizacji, odnoszących się całościowo do problemu ich zabezpieczenia, przetwarzanych w sposób zautomatyzowany jak i niezautomatyzowany.

Polityka Bezpieczeństwa Danych Osobowych stanowi integralny element systemu zarządzania Spółką, wypełniający obowiązki prawne w zakresie dokumentacji procesu przetwarzania danych osobowych.

BezDebetu.pl Sp. z o. o. Sp.k. zapewnia bezpieczeństwo przetwarzania danych osobowych oraz wspiera działania i inicjatywy związane z ochroną zbiorów danych osobowych i systemów informatycznych. Zgodnie z art. 24 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 (w dalszej części zwanego RODO) uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia BezDebetu.pl Sp. z o. o. Sp.k. wdrożyła odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z obowiązującymi przepisami i aby móc to wykazać. Wdrożone środki techniczne i organizacyjne mają na celu zagwarantować zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania danych osobowych w Spółce.

Celem Polityki Bezpieczeństwa jest zabezpieczenie danych osobowych, przetwarzanych na potrzeby Spółki, przed niedozwolonym lub niezgodnym z prawem przetwarzaniem, przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, uszkodzeniem, modyfikacją, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Polityka Bezpieczeństwa określa podstawowe zasady bezpieczeństwa i zarządzania bezpieczeństwem systemów informatycznych oraz dotyczy wszystkich danych osobowych, przetwarzanych na potrzeby Spółki niezależnie od formy ich przetwarzania oraz od tego czy dane są lub mogą być przetwarzane w zbiorach danych.

Treść Polityki oparta została na wymaganiach w tym zakresie zawartych 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 (Dz. Urz. UE L 119/1 z 04.05.2016), zwanemu dalej RODO;
- Ustawie o ochronie danych osobowych z dnia 10 maja 2018 r (Dz.U. z 2018 r. poz. 1000) zwanej dalej Ustawą;
- Ustawie o narodowym zasobie archiwalnym i archiwach z dnia 14 lipca 1983 r. (tekst jednolity Dz. U. z 2018 r. poz. 217);
- Kodeksie pracy z dnia 26 czerwca 1974 r. (tekst jednolity: Dz. U. 2018 poz. 917);
- Kodeksie cywilnym z dnia 23 kwietnia 1964 r. (tekst jednolity: Dz. U. 2018 poz. 1025);
- Ordynacji podatkowej z dnia 29 sierpnia 1997 r. (tekst jednolity: Dz. U. 2018 poz. 800);
- Wyrokach i uchwałach Trybunału Konstytucyjnego, Sądu Najwyższego, Naczelnego i wojewódzkich Sądów Administracyjnych;
- Opiniach i zaleceniach Prezesa Urzędu Ochrony Danych Osobowych;
- PN-ISO-IEC 27001 – Technika informatyczna. Techniki Bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania;
- PN-ISO-IEC 27002 Technika informatyczna - Techniki bezpieczeństwa - Praktyczne zasady zarządzania bezpieczeństwem informacji
- PN-ISO-IEC 27005 – Technika informatyczna. Techniki Bezpieczeństwa. Zarządzanie ryzykiem w bezpieczeństwie informacji;
- PN-ISO 31000 Zarządzanie ryzykiem - Zasady i wytyczne;
- ISO 22301 (BS 25999) Zarządzanie ciągłością działania.

Wdrożone przez Spółkę środki techniczne i organizacyjne mają na celu przetwarzanie danych osobowych zgodnie z zasadami wyrażonymi w art. 5 ust. 1 RODO, tj.:

- **legalności, rzetelności, przejrzystości** – właściwości zapewniającej, że dane przetwarzane są zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dotyczą,
- **ograniczenia celu** – właściwości zapewniającej, że dane są zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami,
- **minimalizacji danych** – właściwości zapewniającej, że zbierane dane są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów , w których są przetwarzane,

- **prawidłowości** – właściwości zapewniającej, że zbierane dane są prawidłowe i w razie potrzeby uaktualniane,
- **ograniczenia przechowywania** – właściwości zapewniającej, że dane przechowywane są w formie umożliwiającej identyfikacje osoby przez okres nie dłuższy niż jest to niezbędne do realizacji celów w których dane te są przetwarzane,
- **poufności** — właściwości zapewniającej, że dane nie są udostępniane nieupoważnionym podmiotom,
- **integralności** — właściwości zapewniającej, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
- **rozliczalności** — właściwości zapewniającej, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

1.1. DEFINICJE

Ilekroć w Polityce jest mowa o:

- **Danych osobowych** – rozumie się przez to 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;
- **Przetwarzaniu danych osobowych** – rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
- **Systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

- **Zbiorze danych osobowych** – rozumie się przez to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
- **Administratorze Danych Osobowych (ADO)** – rozumie się przez to BezDebetu.pl Sp. z o. o. Sp.k. reprezentowaną przez Prezesa Spółki;
- **Administratorze systemu informatycznego (ASI)** – rozumie się przez to informatyka podległego służbowo w zakresie ochrony danych osobowych ADO;
- **Osobie upoważnionej do przetwarzania danych osobowych** – rozumie się przez to osobę, która została upoważniona na piśmie przez ADO do przetwarzania danych osobowych;
- **Użytkowniku** – rozumie się przez to osobę upoważniona do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło do systemu informatycznego;
- **Przetwarzającym** – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu ADO;
- **Odbiorcy danych** – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią zgodnie z zapisami art. 4 ust 1 pkt 9 RODO;
- **Identyfikatorze** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
- **Haśle** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
- **Sieci telekomunikacyjnej** – rozumie się przez to sieć telekomunikacyjną w rozumieniu ustawy z dnia 16 lipca 2004 roku – Prawo telekomunikacyjne (tekst ujednolicony: Dz.U. 2017 poz. 1907);
- **Sieci publicznej** - rozumie się przez to sieć publiczną w rozumieniu ustawy z dnia 16 lipca 2004 roku – Prawo telekomunikacyjne (tekst ujednolicony: Dz.U. 2017 poz. 1907);
- **Raporcie** – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
- **Uwierzytelnianiu** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

Pojęcia użyte, a nieopisane, w niniejszej Polityce należy definiować zgodnie z powszechnie obowiązującym ich znaczeniem słownikowym.

1.2. CEL

Wprowadzenie Polityki Bezpieczeństwa Danych Osobowych w Spółce ma na celu wdrożenie odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie danych osobowych odbywało się zgodnie z obowiązującymi przepisami prawa w tym w szczególności z zapisami RODO.

1.3. KLUCZOWE ZASADY I ZAKRES STOSOWANIA

Polityka Bezpieczeństwa Danych Osobowych Spółki dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny w księgach, wykazach i innych zbiorach ewidencyjnych, jak również w systemach informatycznych. Administratorem wszelkiego rodzaju danych osobowych zapisanych na nośnikach będących własnością Spółki jest Spółka, chyba, że występuje w charakterze przetwarzającego (administrującego) danymi powierzonymi przez podmiot zewnętrzny.

Polityka Bezpieczeństwa Danych Osobowych Spółki realizuje ochronę przetwarzanych zbiorów danych osobowych poprzez zapewnienie zachowania ich bezpieczeństwa. Bezpieczeństwo danych osobowych to określony w niniejszej Polityce i przyjęty do stosowania zbiór norm, zasad, środków i metod ich ochrony, którego miarą jest poziom ryzyka naruszenia ich integralności, rozliczalności, dostępności i poufności. Minimalne wymagania w zakresie bezpieczeństwa danych osobowych zostały wymienione w załączniku nr 1 do niniejszej Polityki.

Bezpieczeństwo danych osobowych jest zapewnione, jeżeli poziom ryzyka naruszenia ich integralności, rozliczalności, dostępności i poufności nie przekracza akceptowalnych parametrów przy zachowaniu zasad określonych w niniejszej Polityce. ADO 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.

ADO przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. ADO analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych, uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o rożnym prawdopodobieństwie wystąpienia i wadze

zagrożenia. ADO dokonuje także oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych.

W celu zapewnienia odpowiedniego poziomu bezpieczeństwa przetwarzanych danych osobowych stosuje się następujące zasady:

- „przywilejów koniecznych" – każdy pracownik posiada uprawnienia ograniczone wyłącznie do tych, które są mu niezbędne i konieczne do wykonywania powierzonych mu obowiązków służbowych;
- „wiedzy koniecznej" – każdy pracownik posiada dostęp do danych osobowych ograniczony wyłącznie do tych, które są mu niezbędne i konieczne do wykonywania powierzonych obowiązków służbowych;
- „indywidualnej odpowiedzialności" – każdy pracownik powinien mieć jednoznacznie określony zakres indywidualnej odpowiedzialności za przetwarzane dane osobowe;
- „czystego biurka" – zabronione jest pozostawianie na stanowisku pracy jakichkolwiek dokumentów lub nośników zawierających dane osobowe po zakończeniu dnia pracy lub w trakcie czasowej nieobecności.

Procedury i zasady określone w niniejszym dokumencie stosuje się do wszystkich osób upoważnionych przez ADO do przetwarzania danych osobowych, zarówno zatrudnionych (bez względu na rodzaj stosunku pracy), jak i innych wykonujących obowiązki na rzecz Spółki, np. praktykantów, stażystów, wolontariuszy.

2. ORGANIZACJA PRZETWARZANIA DANYCH OSOBOWYCH

W celu poprawnej realizacji postanowień niniejszej Polityki wprowadza się poniższy zakres ról i odpowiedzialności w zakresie zapewnienia właściwego procesu zarządzania bezpieczeństwem przetwarzanych danych osobowych.

2.1. ADMINISTRATOR DANYCH OSOBOWYCH (ADO)

Administrator Danych Osobowych reprezentowany przez Prezesa Spółki realizuje zadania w zakresie ochrony przetwarzanych danych osobowych, w tym zwłaszcza:

- podejmuje decyzje o celach i środkach przetwarzania danych osobowych, zwłaszcza z uwzględnieniem zmian w obowiązującym prawie, organizacji Spółki oraz technik zabezpieczania danych osobowych;
- prowadzi oraz aktualizuje dokumentację opisującą sposób przetwarzania danych osobowych,

- uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z obowiązującym prawem;
- nadzoruje udostępnianie danych osobowych odbiorcom danych i innym podmiotom;
- upoważnia poszczególne osoby do przetwarzania danych osobowych w stosownym, indywidualnie określonym zakresie i przechowuje rejestr wydanych upoważnień;
- podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa danych osobowych;
- zatwierdza wzory dokumentów dotyczących ochrony danych osobowych przygotowywane przez pracowników Spółki;
- bez zbędnej zwłoki- w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia - zgłasza organowi nadzorczemu naruszenia ochrony danych osobowych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych,
- jeżeli ww. naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu;
- dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze,
- 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,
- jeżeli ocena skutków dla ochrony danych wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania administrator konsultuje się z organem nadzorczym.

2.2. ADMINISTRATOR SYSTEMU INFORMATYCZNEGO (ASI)

Administrator systemu informatycznego bezpośrednio odpowiada za zarządzanie systemem informatycznym służącym do przetwarzania danych osobowych, a w szczególności:

- zarządza systemem informatycznym, w którym przetwarzane są dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych z pozycji administratora;
- zobowiązany jest do systematycznego kontrolowania i testowania bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym Spółki;
- zobowiązany jest do cyklicznego przeprowadzania audytów w obszarze wybranych procedur bezpieczeństwa danych osobowych;
- przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe;
- przydziela każdemu upoważnionemu użytkownikowi identyfikator oraz hasło do systemu informatycznego, przydział następuje na pisemny wniosek bezpośredniego przełożonego użytkownika;
- nadzoruje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych;
- podejmuje działania w zakresie ustalania i kontroli identyfikatorów dostępu w systemie informatycznym;
- wyrejestrowuje użytkowników oraz zmienia zakresy uprawnień na polecenie ADO;
- w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje ADO o naruszeniu i współdziała z nimi przy usuwaniu jego skutków;
- prowadzi szczegółową dokumentację naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym;
- nadzoruje wykonywanie napraw, konserwacji oraz likwidacji urządzeń komputerowych, na których zapisane są dane osobowe;
- sprawuje nadzór nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego;
- przydziela i rejestruje służbowe komputerowe nośniki informacji.

3. OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

Do przetwarzania danych osobowych może zostać dopuszczona wyłącznie osoba posiadająca imienne, indywidualne upoważnienie wydane przez ADO. Osoba upoważniona może przetwarzać dane osobowe wyłącznie w indywidualnie ustalonym zakresie i tylko w celu wykonywania nałożonych na nią obowiązków na wyraźne polecenie ADO.

Zakres dostępu do danych osobowych przetwarzanych w systemie informatycznym Spółki przypisany jest do niepowtarzalnego identyfikatora użytkownika, niezbędnego do rozpoczęcia pracy w systemie. Rozwiązanie stosunku pracy, odwołanie z pełnionej funkcji, zmiana stanowiska pracy powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych.

Szczególne kategorie danych osobowych mogą być przetwarzane przez – lub na odpowiedzialność – pracownika podlegającego obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe.

Wszyscy upoważnieni do przetwarzania danych zobowiązani są do:

- zapoznania się z przepisami niniejszej Polityki zatwierdzonej przez ADO, mającej na celu zgodne z prawem, w tym zwłaszcza adekwatne do celu przetwarzanie danych osobowych;
- odpowiedniego zabezpieczenia danych przed dostępem do nich osób nieupoważnionych.

4. INFRASTRUKTURA PROCESU PRZETWARZANIA DANYCH OSOBOWYCH

4.1. OBSZAR PRZETWARZANIA DANYCH OSOBOWYCH

Obszar przetwarzania danych osobowych powinien być tak zabezpieczony, aby umożliwić skuteczną ochronę przed nieuprawnionym dostępem, modyfikacją danych, ich uszkodzeniem lub zniszczeniem. Administrator Danych przetwarza dane osobowe w pomieszczeniach zajmowanych przez BezDebetu.pl Sp. z o. o. Sp.k. znajdujących się w Warszawie ul. Powsińska 75 lok 1 oraz w przypadku pracy na odległość w miejscu wykonywania pracy prze pracownika Spółki.

4.2. WYKAZ ZBIORÓW DANYCH OSOBOWYCH

W celu minimalizacji przetwarzanych danych i maksymalnego ograniczenia dostępu zgodnie z zasadą „wiedzy koniecznej" ADO wyodrębnił zbiory danych osobowych posiadane przez Spółkę. Zbiory te ze względu na sposób przetwarzania danych, są zbiorami dualnymi, w których dane osobowe przetwarza się metodą klasyczną i jednocześnie w systemie informatycznym. Zbiory danych osobowych tworzą wyłącznie osoby upoważnione do przetwarzania tych danych, zgodnie z potrzebami realizacji zadań służbowych.

Administrator danych przetwarza dane osobowe wyłącznie w zbiorach i za pomocą aplikacji wskazanych w Wykazie zbiorów danych osobowych, którego wzór stanowi załącznik nr 2 do niniejszej Polityki.

4.3. STRUKTURA ZBIORÓW DANYCH OSOBOWYCH

Zbiory danych osobowych tworzy się według następujących zasad:

- nazwa zbioru powinna odzwierciedlać cel przetwarzania danych osobowych i być zgodna z nazewnictwem stosowanym w przepisach prawa lub winna być określona przez kierownika jednostki organizacyjnej;
- winna być podana podstawa prawna do przetwarzania danych;
- winien być określony sposób i miejsce przetwarzania danych oraz wykaz osób mających do nich dostęp.

Administrator danych przetwarza dane osobowe wyłącznie w zbiorach o strukturze wskazanej w Wykazie zbiorów danych osobowych, którego wzór stanowi załącznik nr 2 do niniejszej Polityki.

4.4. PRZEPŁYW DANYCH POMIĘDZY SYSTEMAMI

Przepływ danych osobowych, pomiędzy systemami informatycznymi zastosowanymi w celu ich przetwarzania, odbywa się w postaci przepływu jednokierunkowego lub przepływu dwukierunkowego. Przepływ jednokierunkowy oznacza, że system informatyczny udostępnia dane ze zbioru (bazy) danych tylko w trybie „do odczytu". Przepływ dwukierunkowy umożliwia upoważnionemu użytkownikowi korzystanie z danych w trybach „do odczytu" i „do zapisu", tj. umożliwia wprowadzanie nowych danych i modyfikację istniejących. Przesyłanie danych pomiędzy systemami informatycznymi może odbywać się sposób manualny, przy wykorzystaniu nośników wymiennych (np. CD, DVD, dysk wymienny, urządzenie typu Pen Drive) lub w sposób półautomatyczny, kiedy po wydaniu polecenia przez upoważnionego użytkownika następuje przeniesienie danych do zbioru za pomocą teletransmisji (np. poprzez lokalną sieć komputerową).

5. BEZPIECZEŃSTWO OSOBOWE

Wszystkie osoby realizujące zadania na rzecz Spółki, bez względu na rodzaj umowy zatrudnienia, odpowiedzialne są za przestrzeganie regulacji zawartych w niniejszej Polityce, za ochronę powierzonych im do przetwarzania danych osobowych oraz elementów systemu informatycznego.

ADO ma obowiązek zapoznać pracownika z jego zakresem odpowiedzialności dotyczącym kwestii bezpieczeństwa danych osobowych. Zakres ten musi być ujęty w postaci odpowiednich zapisów w posiadanym przez pracownika zakresie obowiązków.

Pracownik musi zostać zapoznany z zasadami odpowiedzialności dyscyplinarnej i karnej związanej z nieprzestrzeganiem zasad bezpieczeństwa danych osobowych.

5.1. REKRUTACJA

Celem procesu weryfikacji kandydatów do pracy w Spółce jest ograniczenie ryzyka błędu ludzkiego, kradzieży, oszustwa, sabotażu lub niewłaściwego postępowania z informacjami chronionymi poprzez zweryfikowanie tożsamości rekrutowanych pracowników oraz ich umiejętności zawodowych. Podczas rekrutacji pracowników weryfikacji podlega kompletność i rzetelność informacji przedstawionych przez kandydata, w szczególności dotyczących jego wykształcenia, posiadanych kwalifikacji i dotychczasowego przebiegu zatrudnienia.

Na etapie rekrutacji Spółka może żądać od kandydata do pracy następujących danych:

- Imię (imiona) i nazwisko,
- Imiona rodziców,
- Data urodzenia
- Miejsce zamieszkania (adres do korespondencji),
- Wykształcenie,
- Przebieg dotychczasowego zatrudnienia.

W przypadku innego rodzaju danych osobowych ich podanie jest całkowicie dobrowolne przez kandydata i wymaga udzielenia pisemnej lub elektronicznej zgody na ich przetwarzanie. W celu realizacji obowiązku informacyjnego w ogłoszeniu o pracę zamieszcza się informację o ADO dla kandydata, której wzór stanowi załącznik nr 3.

Wszyscy pracownicy, ze szczególnym zwróceniem uwagi na osoby mające bezpośredni dostęp do przetwarzanych zbiorów danych osobowych, dobierani są z uwzględnieniem takich cech kandydata jak uczciwość, odpowiedzialność oraz przewidywalność zachowań.

W trakcie procesu rekrutacji tworzy się w Spółce zbiór zawierający dane osobowe kandydatów do pracy pod nazwą „CV". Po zakończeniu procedury naboru dane osobowe nowozatrudnionych pracowników przenoszone są do zbioru danych osobowych „Pracownicy". Oryginały niewykorzystanych dokumentów odsyłane są kandydatom do pracy listem poleconym. CV zawierające zgodę na dalsze procesy rekrutacyjne pozostają w Spółce. CV zawierające zgodę tylko na konkretną rekrutację zostają komisyjnie zniszczone po zakończeniu procesu rekrutacji. Zniszczenie dokumentów potwierdzone jest protokołem.

5.2. PRACOWNICY

Od osoby zatrudnionej w ramach umowy o pracę Spółka oprócz informacji wymienionych w pkt. 5.1. Polityki może żądać również:

- innych danych osobowych pracownika, w tym imion i nazwisk oraz dat urodzenia dzieci pracownika, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy;
- numeru PESEL pracownika nadanego przez Rządowe Centrum Informatyczne Powszechnego Elektronicznego Systemu Ewidencji Ludności (RCI PESEL);
- numer rachunku płatniczego, jeżeli pracownik nie złożył wniosku o wypłatę wynagrodzenia do rąk własnych (obowiązuje od 01.09.2019 r.)

Przy podpisywaniu umowy o pracę pracownikowi jest wręczana informacja o administratorze danych, której wzór stanowi załącznik nr 3.

Wszelkie inne informacje dodatkowe mogą być przetwarzane na podstawie pisemnej zgody udzielonej przez Pracownika.

5.3. STARZYŚCI, PRAKTYKANCI, WOLONTARIUSZE

Należy zapewnić, aby stażyści, praktykanci oraz wolontariusze wykonujący pracę w strukturach Spółki przeszli szkolenie z zakresu ochrony danych osobowych zakończone podpisaniem oświadczenia o znajomości przepisów i wydaniem upoważnienia. W przeciwnym wypadku należy zorganizować szczególny nadzór nad wykonywanymi przez nich czynnościami związanymi z dostępem do zasobów informacyjnych, w szczególności przetwarzanych w systemie informatycznym.

5.4. ZOBOWIĄZANIE DO ZACHOWANIA POUFNOŚCI

Pracownicy Spółki, bez względu na formę zatrudnienia, zobowiązani są do podpisania oświadczenia potwierdzającego zapoznanie się z zasadami określonymi w niniejszej Polityce, zobowiązania dotyczącego zachowania poufności danych osobowych oraz odpowiedzialności wynikającej z przepisów RODO. Wzór oświadczenia stanowi Załącznik nr 4 do niniejszej Polityki.

Podpisanie oświadczenia przez pracownika oznacza przyjęcie odpowiedzialności za podejmowane działania. Odpowiedzialność pracowników za ochronę powierzonych im danych osobowych zgodnie z zasadami określonymi w niniejszej Polityce rozciąga się także poza siedzibę Spółki i poza normalne godziny pracy. Odpowiedzialność pracownika rozciąga się również na okres po ustaniu stosunku pracy.

Delegowanie uprawnień na podległych pracowników nie zdejmuje odpowiedzialności za dbałość o bezpieczeństwo danych osobowych z osoby dokonującej delegacji uprawnień.

6. UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

Do przetwarzania danych osobowych w Spółce mogą być dopuszczone wyłącznie osoby posiadające indywidualne upoważnienie nadane przez ADO. Upoważnienie do przetwarzania danych osobowych musi być każdorazowo sporządzone w formie pisemnej i zawierać jasno sprecyzowany zakres i czas obowiązywania. Upoważnienie do przetwarzania danych osobowych nie może być zastąpione upoważnieniem wynikającym ze stosunku prawnego łączącego osobę ze Spółką (np. umowa o dzieło). Niedopuszczalne jest udzielenie dostępu do danych osobowych przed zakończeniem formalnej procedury upoważnienia. Zakaz przetwarzania danych osobowych przez osoby nieposiadające upoważnień jest bezwzględny.

Kwestia nadawania upoważnień do przetwarzania danych osobowych w zbiorach przekazanych podmiotom zewnętrznym do przetwarzania lub przyjętych do przetwarzania od tych podmiotów uregulowana jest w odrębnej procedurze opisanej w rozdziale 14 niniejszej Polityki.

6.1. NADAWANIE UPOWAŻNIEŃ

Każdy pracownik Spółki działający z upoważnienia administratora i mający dostęp do danych osobowych przetwarza je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego i wyłącznie w zakresie sprecyzowanym w nadanym mu upoważnieniu. Zakres uprawnień danej osoby określony jest zgodnie z zakresem obowiązków na zajmowanym przez tą osobę stanowisku pracy. Polecenie ADO musi mieć formę pisemną, może stanowić odrębny dokument zgodnie z załącznikiem nr 5 lub być częścią umowy podpisanej z ADO (np. umowy o prace, umowy powierzenia).

Dostęp do danych osobowych przetwarzanych przez Spółkę może być udzielony tylko osobie o zweryfikowanej tożsamości. ADO decyzje o nadaniu upoważnienia do przetwarzania danych osobowych. Upoważnienie powinno mieć formę pisemną. Wzór upoważnienia stanowi Załącznik nr 6 do niniejszej Polityki.

Powyższe zasady odnoszą się bezpośrednio także do procedury zmiany nadanych upoważnień.

Upoważnienia są rejestrowane i przechowywane przez ADO. Wzór rejestru wydanych upoważnień stanowi Załącznik nr 7 do niniejszej Polityki.

6.2. ODBIERANIE I WYGAŚNIĘCIE UPOWAŻNIENIA

Odebranie upoważnienia do przetwarzania danych osobowych (całkowite bądź czasowe) jest decyzją ADO. Odebranie upoważnienia do przetwarzania danych osobowych osobie posiadającej dostęp do systemu informatycznego następuje poprzez bezzwłoczne zablokowanie konta.

Wygaśnięcie upoważnienia do przetwarzania danych osobowych następuje z datą określoną na upoważnieniu lub z chwilą rozwiązania umowy o pracę lub innego stosunku cywilno-prawnego z osobą upoważnioną.

Zalecane jest czasowe odbieranie upoważnienia do przetwarzania danych osobowych w sytuacji:

- wszczęcia wobec użytkownika postępowania dyscyplinarnego;
- zawieszenia użytkownika w pełnieniu obowiązków służbowych;
- wypowiedzenia użytkownikowi umowy o pracę.

6.3. UDZIELANIE DOSTĘPU DO DANYCH OSOBOWYCH DLA OSÓB „Z ZEWNĄTRZ"

Udzielenie osobie „z zewnątrz" praw dostępu do danych osobowych przetwarzanych w Spółce musi być podyktowane faktyczną potrzebą, niezbędną do normalnego funkcjonowania, lub wymaganą w celu realizacji wymagań prawnych. Nadanie dostępu odbywa się na polecenie ADO, wyłącznie w zakresie określonym w upoważnieniu. Osobom „z zewnątrz" dane osobowe należy udostępniać tylko w niezbędnym zakresie i tylko w niezbędnej ilości po podpisaniu przez nie oświadczenia potwierdzającego zapoznanie się z zasadami określonymi w niniejszej Polityce oraz zobowiązania dotyczącego zachowania poufności danych osobowych oraz świadomość odpowiedzialności wynikającej z zapisów RODO.

Dopuszczenie do danych osobowych i systemu informatycznego Spółki mające na celu realizację wymagań prawa może być realizowane tylko w granicach wyznaczonych przez dane przepisy.

Zalecane jest przeprowadzenie analizy skutków dopuszczenia osób „z zewnątrz" do zasobów zbiorów danych osobowych i systemu informatycznego Spółki, w celu oszacowania zagrożeń i zastosowania odpowiednich środków zaradczych. Przy szacowaniu ryzyka należy wziąć pod uwagę rodzaj wymaganego dostępu, rodzaj danych, zabezpieczenia stosowane przez osoby „z zewnątrz" oraz wpływ udzielonego dostępu na bezpieczeństwo danych osobowych przetwarzanych przez Spółkę.

Udzieleniem dostępu do danych osobowych dla osób „z zewnątrz" jest nie tylko fizyczne ich dopuszczenie do pomieszczeń, w których przetwarzane są dane osobowe, udostępnienie

dokumentów czy dostęp do systemu informatycznego, ale także przekazanie informacji ustnej czy pisemnej uprawnionym organom państwowym oraz klientom i kontrahentom.

Procedura nadawania upoważnień do przetwarzania danych osobowych dla osób „z zewnątrz" jest tożsama z procedurą dla pracowników Spółki.

6.4. UDOSTĘPNIANIE INFORMACJI „NA ZEWNĄTRZ"

Przekazywanie poza Spółkę danych osobowych może nastąpić tylko w sytuacji możliwości bezpośredniej identyfikacji i potwierdzenia tożsamości Odbiorcy. W razie wątpliwości zgodę na przekazanie danych osobowych Odbiorcom danych podejmuje osobiście ADO.

Należy do niezbędnego minimum ograniczyć możliwość ustnego przekazywania „na zewnątrz" jakichkolwiek informacji, bez względu na subiektywne przekonanie o identyfikacji i potwierdzeniu tożsamości Odbiorcy.

7. SZKOLENIA

Poziom wiedzy pracowników Spółki, niezbędny dla zapewnienia bezpieczeństwa informacji, należy utrzymywać poprzez możliwie regularny udział w seminariach, kursach i szkoleniach.

Wszyscy pracownicy Spółki przed udzieleniem dostępu do danych osobowych, a w szczególnych przypadkach także osoby trzecie, muszą przejść właściwe, okresowo uaktualniane przeszkolenie w zakresie zasad określonych w niniejszej Polityce. Za realizację i uaktualnianie szkoleń odpowiada ADO.

Częstotliwość szkoleń określa ADO. Szkolenia w zakresie bezpieczeństwa informacji prowadzone są przez osobę wyznaczoną przez ADOD, posiadającą odpowiednią wiedzę i doświadczenie w zakresie ochrony danych osobowych.

Do realizacji szkoleń można wykorzystać zewnętrzne specjalistyczne firmy szkoleniowo-doradcze.

Osoby przeszkolone poświadczają własnoręcznym podpisem fakt udziału w szkoleniu i zapoznanie z aktualnymi procedurami bezpieczeństwa obowiązującymi w Spółce.

7.1. ZAKRES TEMATYCZNY SZKOLEŃ

Tematyka szkoleń w zakresie ochrony danych osobowych w szczególności powinna obejmować:

- krótką prezentację obowiązujących w RP uregulowań prawnych w zakresie ochrony danych osobowych;
- zasady i procedury określone w Polityce;

- schemat organizacyjny ochrony danych osobowych w Spółce;
- przedstawienie najnowszych rozwiązań w zakresie organizacyjno - technicznego bezpieczeństwa informacji;
- prawa i obowiązki osób upoważnionych;
- procedury dostępu do systemu informatycznego służącego do przetwarzania danych osobowych;
- przedstawienie zagrożeń dla bezpieczeństwa danych osobowych przetwarzanych w Spółce oraz metod i środków ich ograniczenia;
- zasady postępowania w przypadku naruszenia bezpieczeństwa danych osobowych;
- odpowiedzialność karną, dyscyplinarną, administracyjną i cywilną za nieprzestrzeganie zasad ochrony danych osobowych;

8. KONTROLA DOSTĘPU

Za kontrolę dostępu do pomieszczeń, w których przetwarzane są dane osobowe odpowiedzialne są osoby upoważnione do ciągłego w nich przebywania, tj. pracownicy wykonujący zadania w tych pomieszczeniach. Niedopuszczalne jest pozostawianie „osób trzecich" w pomieszczeniach, w których przetwarzane są dane osobowe bez nadzoru osób upoważnionych, jak również umożliwianie dostępu do tych pomieszczeń podczas swojej nieobecności. Odpowiedzialność dyscyplinarną za niedopełnienie wskazanych obowiązków ponoszą osoby odpowiedzialne za pomieszczenie.

9. BEZPIECZEŃSTWO DOKUMENTACJI TRADYCYJNEJ

Wszelkiego rodzaju dokumenty tradycyjne zawierające dane osobowe należy bezwzględnie zabezpieczyć przed ich niedozwolonym lub niezgodnym z prawem przetwarzaniem, przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, uszkodzeniem, modyfikacją, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem do zawartych w nich danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. Zabrania się powtórnego używania do sporządzania brudnopisów pism jednostronnie zadrukowanych, jeśli zawierają one dane osobowe. Akta lub pojedyncze dokumenty zawierające dane osobowe należy przechowywać w przeznaczonych do tego celu szafach zamykanych na klucz lub w zabezpieczonych pomieszczeniach.

Dokumentacje tradycyjna należy szczególnie zabezpieczyć przed działalnością czynników środowiskowych mogących spowodować ich zniszczenie lub nieczytelność.

Wydruki zawierające dane osobowe, po wykorzystaniu, należy codziennie przed zakończeniem pracy zniszczyć w niszczarce (zalecana klasa DIN3). Kategorycznie zabrania się wyrzucać wydruki zawierające dane osobowe do koszy na śmieci.

10. BEZPIECZEŃSTWO ZASOBÓW SPRZĘTOWYCH

Urządzenia systemu informatycznego Spółki muszą spełniać wymogi oraz poziom bezpieczeństwa określony przez niniejszą Politykę oraz wypracowane na jej podstawie regulacje szczegółowe i wymogi prawne w tym zakresie. Sprzęt służący do przetwarzania danych osobowych musi być należycie chroniony przed zagrożeniami dla jego bezpieczeństwa i wpływem niebezpiecznych czynników środowiskowych.

ADO wykazuje szczególną staranność przy zabezpieczeniu danych osobowych przetwarzanych w systemach informatycznych Spółki na wypadek wystąpienia sytuacji losowych lub nieprzewidzianego oddziaływania czynników zewnętrznych na zasoby systemu, jak np.: pożar, zalanie pomieszczeń, katastrofa budowlana, napad, kradzież, włamanie, niewłaściwe parametry środowiska zakłócające prace urządzeń komputerowych, jak nadmierna wilgotność lub bardzo wysoka temperatura, oddziaływanie pola elektromagnetycznego i inne.

Użytkowanie zasobów sprzętowych systemu informatycznego Spółki odbywa się zgodnie z zaleceniami producentów i dostawców oraz warunkami gwarancji.

10.1. DOSTĘP DO SYSTEMU INFORMATYCZNEGO

W celu poprawnej realizacji zasad bezpieczeństwa przetwarzanych danych osobowych w systemie informatycznym Spółki niezbędne jest właściwe zarządzanie prawami dostępu do systemu, jego zasobów i aplikacji. Żaden pracownik lub osoba „z zewnątrz" nie może uzyskać dostępu do zasobów sieciowych, aplikacji lub systemów bez formalnego przeprowadzenia procedury nadania uprawnień dostępu do systemu informatycznego.

Formalny dostęp do systemu informatycznego i jego poszczególnych elementów jest uzasadniony potrzebami organizacyjnymi i biznesowymi Spółki. Nie może on wykraczać poza obowiązki oraz potrzeby określone dla danego stanowiska pracy. Dostęp do systemu informatycznego Spółki otrzymuje jedynie osoba uprzednio zapoznana z niniejszą Polityką i przeszkolona w zakresie podstawowych zasad bezpiecznego korzystania z komputera.

10.2.PRZYDZIELANIE DOSTĘPU DO SYSTEMU

Dostęp do systemu informatycznego może być udzielony tylko osobie o zweryfikowanej tożsamości, posiadającej nadane przez ADO upoważnienie do przetwarzania danych osobowych.

Przetwarzanie danych osobowych w systemie informatycznym odbywa się wyłącznie na polecenie ADO. Zakres uprawnień danego użytkownika jest określany zgodnie z zakresem obowiązków i dokładnie sprecyzowany w upoważnieniu do przetwarzania danych osobowych. Niedopuszczalne jest udzielenie dostępu do systemu informatycznego przed zakończeniem formalnej procedury przydzielenia uprawnień. Nadanie uprawnień dostępu do systemu informatycznego kończy się wprowadzeniem danych upoważnionej osoby do bazy użytkowników i nadaniem identyfikatora pozwalającego na jego identyfikację i uwierzytelnienie.

Uprawnienia dostępu do systemu informatycznego Spółki osobom „z zewnątrz" mogą być nadane wyłącznie na czas niezbędny do realizacji określonych celów i możliwie ograniczone.

10.2.1. ODBIERANIE DOSTĘPU DO SYSTEMU

Odebranie dostępu do systemu informatycznego realizowane jest przez ASI na polecenie ADO.

Odebranie dostępu może być także autonomiczną decyzją ASI w sytuacji stwierdzenia naruszenia zasad bezpieczeństwa systemu informatycznego. Odebranie praw dostępu do systemu informatycznego może mieć charakter czasowy lub trwały. Odebranie praw dostępu następuje poprzez bezzwłoczne zablokowanie konta. Usunięcie konta może nastąpić dopiero po okresie 1 roku od jego zablokowania.

Zalecane jest czasowe odbieranie praw dostępu do systemu informatycznego w sytuacji:

- nieobecności użytkownika w pracy trwającej dłużej niż 1 miesiąc;
- wszczęcia wobec użytkownika postępowania dyscyplinarnego;
- zawieszenia użytkownika w pełnieniu obowiązków służbowych;
- wypowiedzenia użytkownikowi umowy o pracę.

10.2.2. UWIERZYTELNIANIE UŻYTKOWNIKÓW SYSTEMU

Podstawowym mechanizmem uwierzytelniania użytkowników systemu informatycznego jest unikalny identyfikator oraz powiązane z nim hasło dostępu.

Dopuszczalne jest zastąpienie użytkowania hasła poprzez zastosowanie odpowiednio silnych technik opartych na urządzeniach uwierzytelniających lub metodach biometrycznych.

10.2.3. IDENTYFIKACJA UŻYTKOWNIKÓW

Wszyscy użytkownicy systemu informatycznego muszą posiadać indywidualne, unikalne identyfikatory przeznaczone do osobistego i wyłącznego użytku. Identyfikator użytkownika nie

może w jakikolwiek sposób wskazywać na jego poziom uprawnień. Identyfikatorów wcześniej wykorzystywanych nie wolno przydzielać innym użytkownikom.

Zaleca się stosowanie jednolitej metodyki tworzenia identyfikatorów dla wszystkich użytkowników systemu informatycznego. Należy, jeżeli to możliwe, posługiwać się jednym identyfikatorem we wszystkich systemach, do których użytkownik otrzymał prawa dostępu.

Dopuszczalne jest stosowanie identyfikatorów grupowych, wyłącznie do zasobów systemu niezawierających danych osobowych.

10.2.4. HASŁA DOSTĘPU

System informatyczny musi zapewniać:

- użycie indywidualnych haseł umożliwiających realizację zasady rozliczalności;
- wymuszanie zmiany haseł tymczasowych przy pierwszym logowaniu;
- uniemożliwienie wyświetlania haseł podczas ich wprowadzania;
- przechowywanie haseł w systemie w formie zaszyfrowanej;
- określenie minimalnej długości i złożoności haseł (hasło skomplikowane, o długości co najmniej 8 znaków);
- wymuszanie zmiany hasła co 180 dni;
- ograniczenie możliwości ponownego użycia wcześniej stosowanych 3 haseł.

ADO po przeanalizowaniu ryzyka związanego z ujawnieniem hasła przez użytkowników zezwolił na zmianę hasła co 180 dni celem zmniejszenia prawdopodobieństwa zapisywania haseł przez użytkowników systemu.

Zabronione jest użytkowanie domyślnych haseł systemowych oprogramowania i sprzętu.

Użytkownik systemu informatycznego ma obowiązek stosować hasła trudne do odgadnięcia. W szczególności hasła nie mogą być:

- związane z życiem zawodowym i osobistym użytkownika (np. numer rejestracyjny samochodu, PESEL, NIP, numer telefonu, nazwisko, imię, adres, itp.);
- słowem w żadnym popularnym języku;
- nazwą geograficzną, terminem technicznym lub określeniem potocznym;
- sekwencją kolejnych znaków na klawiaturze;
- dowolnym spośród wymienionych uzupełnionym na początku lub końcu cyfrą lub liczbą.

Ponadto hasło musi spełniać niżej wymienione warunki:

- długość, co najmniej 8 znaków;
- zawierać wielkie i małe litery;
- zawierać cyfry lub znaki specjalne.

Bezwzględnie zabrania się użytkownikom systemu informatycznego ujawniania, udostępniania i zapisywania haseł dostępu.

Jeżeli istnieje uzasadnione podejrzenie, że hasło zostało ujawnione, należy je natychmiast zmienić, powiadamiając o tym fakcie ASI.

Zabrania się wykorzystywania przez osoby upoważnione nadanego im identyfikatora i hasła do uwierzytelniania w jakichkolwiek zewnętrznych usługach internetowych.

Użytkownik ponosi pełną odpowiedzialność za naruszenie bezpieczeństwa systemu informatycznego przy wykorzystaniu przydzielonego mu identyfikatora i hasła.

10.3. PROCEDURY STACJI ROBOCZYCH

10.3.1. ROZPOCZĘCIE PRACY

Rozpoczęcie pracy na stacji roboczej następuje po włączeniu komputera, a następnie wprowadzeniu indywidualnego, znanego tylko użytkownikowi hasła i identyfikatora.

Dokonując uwierzytelniania w systemie informatycznym należy zwrócić szczególną uwagę by osoby nieuprawnione nie weszły w posiadanie wprowadzanego hasła.

10.3.2. ZAWIESZENIE PRACY

Właściwości monitorów stacji roboczych należy ustawić tak by wygaszacze ekranu uruchamiały się po 15 minutach od przerwania pracy. Wznowienia wyświetlania na ekranie następuje dopiero po wprowadzeniu hasła.

W przypadku opuszczania stanowiska pracy użytkownik zobowiązany jest aktywować wygaszasz ekranu lub w inny sposób zablokować stację roboczą.

Niedopuszczalne jest pozostawianie niewylogowanej stacji roboczej bez osobistego nadzoru, nawet w przypadku chwilowego opuszczenia pomieszczenia, w szczególności gdy pozostają w nim postronne osoby.

10.3.3. ZAKOŃCZENIE PRACY

Zakończenie pracy na stacji roboczej następuje po zapisaniu danych, prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera.

Kategorycznie zabronione jest wyłączenie zasilania stacji roboczej przed wykonaniem czynności wylogowania z systemu, jak również pozostawianie włączonej stacji roboczej (nawet wylogowanej z systemu) po zakończeniu dnia pracy.

10.4. KONTROLA DOSTĘPU DO SYSTEMU

10.4.1. MONITOROWANIE DOSTĘPU DO ZASOBÓW SIECIOWYCH

Wszelkie próby uwierzytelniania użytkowników w systemie informatycznym muszą być rejestrowane oraz muszą umożliwiać identyfikację miejsca, z którego użytkownik uzyskał dostęp.

Każdorazowe uzyskanie dostępu do systemu informatycznego musi być poprzedzone poprawnym uwierzytelnieniem użytkownika. Procedura uwierzytelnienia musi obejmować wymianę informacji jedynie niezbędnej do przeprowadzenia tego procesu. W szczególności podczas uwierzytelniania, jeżeli to możliwe, nie powinny być udostępniane informacje o systemie i aplikacji. W przypadku niepowodzenia uwierzytelniania, system powinien wyświetlać ogólny komunikat o błędzie, bez podania przyczyn niepowodzenia.

Jeżeli to możliwe, system informatyczny ogranicza możliwość jednoczesnej wielokrotnej rejestracji tego samego użytkownika.

System informatyczny musi być dodatkowo wyposażony w mechanizmy ograniczające liczbę nieudanych prób rejestracji. Blokowanie konta użytkownika powinno następować po przekroczeniu pięciu nieudanych prób rejestracji. System informatyczny musi rejestrować wszystkie nieudane próby rejestracji.

10.4.2. MONITOROWANIE DOSTĘPU DO APLIKACJI

Nadawanie użytkownikom dostępu do aplikacji powinno bazować na wcześniej określonych profilach dostępu typowych dla poszczególnych stanowisk pracy. Określenie profili dla poszczególnych stanowisk pracy powinno pokrywać się z zakresem obowiązków na danym stanowisku.

Podczas nadawania uprawnień użytkownikom systemu lub tworzenia profili dostępu należy zwrócić szczególną uwagę na przestrzeganie zasady „wiedzy koniecznej". Użytkownicy nie powinni otrzymywać dostępu do zasobów, które nie są im potrzebne do realizacji obowiązków służbowych.

10.4.3. MONITOROWANIE SYSTEMU

System informatyczny musi być wyposażony w mechanizmy pozwalające na monitorowanie i rejestrowanie zdarzeń, a jednocześnie tak skonfigurowany, aby mógł zapewnić kompletną i wiarygodną rejestrację, bez możliwości ingerencji użytkowników.

Rejestrowane muszą być co najmniej, następujące zdarzenia:

- uprawnione i nieuprawnione próby dostępu zarówno do systemu, jak i bezpośrednio do jego danych;
- uruchomienie i zatrzymanie systemu;
- dołączenie i odłączenie urządzeń wejścia/wyjścia;
- awarie zgłaszane przez procesy lub urządzenia;
- komunikaty o próbach uzyskania dostępu do urządzeń sieciowych lub innych urządzeń umożliwiających dostęp do systemu;
- komunikaty o zidentyfikowanym oprogramowaniu szkodliwym.

Rejestrowanie zdarzeń takich jak próba/uzyskanie dostępu lub wyrejestrowanie z systemu obejmuje:

- identyfikator użytkownika;
- identyfikator stacji roboczej;
- data i czas rejestracji w systemie i wyrejestrowania z systemu;
- zapisy o udanych i nieudanych próbach dostępu do systemu, danych i innych zasobów;
- użyte programy, raporty, dostęp do urządzeń wejścia/wyjścia.

System informatyczny musi być wyposażony w mechanizmy automatycznie rejestrujące operacje na danych, takie jak:

- datę i czas wprowadzenia, zmiany, usunięcia danych osobowych;
- identyfikator użytkownika dokonującego operacji na danych osobowych;
- wartości przed i po dokonaniu zmiany – jeżeli to możliwe;

oraz umożliwiać odnotowanie:

- źródła danych osobowych, w przypadku zbierania danych nie od osoby, której one dotyczą;
- informacje o odbiorcach, którym dane te zostały udostępnione;
- sprzeciwu wobec przetwarzania, złożonego przez osobę, której dane dotyczą.

Dla poprawnej realizacji procesu monitorowania systemu informatycznego niezbędne jest, aby wszystkie urządzenia pracujące w systemie miały zsynchronizowany czas i datę systemową.

10.4.4. DOSTĘP DO SIECI PUBLICZNEJ - INTERNET

System informatyczny Spółki posiada połączenie z siecią publiczną – Internet. Dostęp do niego jest jednak ograniczony i odpowiednio zabezpieczony.

Korzystanie z zasobów informacyjnych sieci publicznej – Internet, za pośrednictwem systemu informatycznego Spółki ma na celu podniesienie skuteczności wypełniania obowiązków służbowych. Zabrania się użytkownikom korzystać z rozwiązań uniemożliwiających lub utrudniających ograniczanie i monitorowanie ich dostępu do sieci publicznej.

10.5. OGRANICZENIA DOSTĘPU

Ze względów bezpieczeństwa systemu informatycznego oraz realizacji przepisów prawa w tym zakresie ASI wprowadza ograniczenia dostępu do niektórych usług internetowych, a w szczególności:

- oprogramowania umożliwiającego wymianę plików typu „p-2-p”;
- niezabezpieczonych komunikatorów internetowych;
- witryn o tematyce pornograficznej, nazistowskiej, propagującej przemoc i nienawiść na tle rasowym;
- płatnych serwisów internetowych.

10.5.1. DOSTĘP DO POCZTY ELEKTRONICZNEJ

Pracownicy Spółki mają przydzielane indywidualne konta pocztowe służące do prowadzenia korespondencji przy wykorzystaniu sieci publicznej – Internet, tzw. poczty elektronicznej e-mail. Konta poczty elektronicznej udostępniane są pracownikom Spółki wyłącznie do wypełniania obowiązków służbowych. Kategorycznie zabrania się używania do wypełniania obowiązków służbowych poczty elektronicznej innej niż zarządzana przez Spółkę, w szczególności komercyjnych niezabezpieczonych portali pocztowych.

Dopuszczalne jest zakładanie zbiorczych skrzynek pocztowych, z dostępem dla wielu osób, za akceptacją ADO.

Pocztę elektroniczną wysyłaną poza Spółkę należy opatrzyć oświadczeniem o jej poufności, o treści zatwierdzonej przez ADO. Informacje stanowiące dane osobowe przed wysłaniem pocztą elektroniczną należy uprzednio zaszyfrować, przy użyciu metod wskazanych w niniejszej Polityce. Zakazane jest przesyłanie pocztą elektroniczną całych baz danych lub ich obszernych wypisów. Wiadomości pocztowe a także ich załączniki, które mogą stanowić zagrożenie dla bezpieczeństwa systemu informatycznego należy usuwać z serwera pocztowego. Przepływ informacji pomiędzy

systemem informatycznym, a siecią publiczną – Internetem zabezpieczony jest oprogramowaniem antyspamowym.

10.6. KOMPUTEROWE NOŚNIKI INFORMACJI

Generalną zasadą przetwarzania danych osobowych jest ich przechowywanie na serwerze obsługującym system informatyczny Spółki. Wskazane jest, aby wszelkie dane osobowe przetwarzane w pamięciach poszczególnych stacji roboczych były niezwłocznie umieszczane na serwerze.

W uzasadnionych przypadkach dopuszcza się incydentalne korzystanie z innych nośników informacji niż służbowe komputerowe nośniki informacji. W przypadku wykorzystywania takiego nośnika w systemie informatycznym Spółki niezbędne jest sprawdzenie go programem antywirusowym. Sprawdzenie ma na celu wyeliminowanie zakażenia systemu informatycznego Spółki wirusami, koniami trojańskimi lub innym złośliwym oprogramowaniem.

Osoby upoważnione do przetwarzania danych osobowych w systemie informatycznym Spółki zobowiązane są do bezwzględnego wypełniania zasad bezpiecznego korzystania z komputerowych nośników informacji.

Przydzielenie pracownikowi komputerowego nośnika informacji musi być podyktowane faktyczną potrzebą organizacyjną, zgodnie z zakresem obowiązków służbowych. Pracownicy, którym przydzielone zostały komputerowe nośniki informacji zostają uświadomieni co do występowania dodatkowego ryzyka związanego z charakterystyką tych urządzeń.

10.6.1. ZASADY KORZYSTANIA Z NOŚNIKÓW

Zakazuje się przetwarzania informacji prawnie chronionych na zewnętrznych nośnikach danych bez ich uprzedniego zaszyfrowania.

Na nośnikach danych dopuszczalne jest przetwarzanie jedynie jednostkowych danych osobowych. Nośniki danych z zaszyfrowanymi, jednostkowymi danymi osobowymi, należy, na czas ich użyteczności, bezwzględnie przechowywać w zamkniętych na klucz szafach, a po ich wykorzystaniu dane w nich zawarte trwale usuwać lub nośniki te zniszczyć.

Nośniki danych należy przechowywać w miejscach, do których dostęp mają wyłącznie osoby upoważnione. Zakazane jest wynoszenie poza pomieszczenia Spółki nośników danych zawierających zbiory danych osobowych.

10.7. KOPIE BEZPIECZEŃSTWA

W celu zapewnienia niezbędnego poziomu bezpieczeństwa zbiorów danych osobowych przetwarzanych w systemie informatycznym Spółki, w szczególności ochrony przed nieuprawnioną modyfikacją lub zniszczeniem, stosuje się obowiązek tworzenia kopii bezpieczeństwa zbiorów danych. Za realizację kopii bezpieczeństwa informacji znajdujących się w zasobach serwerów odpowiada ASI. Częstotliwość wykonywania kopii bezpieczeństwa określa ASI indywidualnie w odniesieniu do każdej z baz danych.

W przypadku każdej aktualizacji systemu lub czynności serwisowej należy wykonać kopie bezpieczeństwa, jeżeli standardowa częstotliwość tworzenia kopii jest większa niż jeden dzień lub jeżeli stosuje się metodę przyrostową.

10.7.1. PRZECHOWYWANIE NOŚNIKÓW KOPII BEZPIECZEŃSTWA

Przyjmuje się, że podstawową metodą przechowywania kopii bezpieczeństwa jest ich tworzenie na zewnętrznych nośnikach informacji, oznaczonych odpowiednio do ich zawartości. W przypadku tworzenia kopii bezpieczeństwa na nośnikach optycznych (CD/DVD) każdą kopię przechowuje się na oddzielnym nośniku.

Nośniki kopii bezpieczeństwa przechowuje się w sposób minimalizujący zagrożenie ze strony sił przyrody oraz silnego pola elektromagnetycznego. Zabrania się przechowywania kopii bezpieczeństwa w pomieszczeniach przeznaczonych do przechowywania zbiorów danych pozostających w bieżącym użytkowaniu. Dostęp do kopii bezpieczeństwa może mieć wyłącznie ASI.

10.7.2. TESTOWANIE KOPII BEZPIECZEŃSTWA

ASI odpowiedzialny jest za okresowe testowanie wybranych kopii bezpieczeństwa, mające na celu ocenę ich przydatność do odtworzenia zasobów systemu w przypadku jego awarii. Stwierdzenie utraty przez kopie zapasowe waloru przydatności do celu, upoważnia ASI do ich zniszczenia.

Testowanie kopii bezpieczeństwa może być przeprowadzane wyłącznie w środowisku komputerowym oddzielonym fizycznie od pracującego systemu informatycznego.

10.7.3. ODZYSKIWANIE DANYCH Z KOPII BEZPIECZEŃSTWA

Odzyskiwanie danych z kopii bezpieczeństwa przeprowadza ASI na polecenie ADO.

10.7.4. LIKWIDACJA KOPII BEZPIECZEŃSTWA

Kopie zapasowe, które zostały przeznaczone do likwidacji pozbawia się zapisu danych osobowych poprzez nadpisanie danych „ciągiem zer" a następnie „ciągiem jedynek" w cyklu trzykrotnym, przy użyciu odpowiedniego oprogramowania.

Uszkodzone kopie zapasowe, dyski lub inne elektroniczne nośniki informacji, które zawierają dane osobowe należy niszczyć mechanicznie, w sposób uniemożliwiający ich ponowne użycie.

Czynności likwidacji kopii oraz niszczenia nośników wykonuje ASI.

10.8. ZABEZPIECZENIA PRZED SZKODLIWYM OPROGRAMOWANIEM

Całe oprogramowanie wykorzystywane przez Spółkę pochodzi z legalnego źródła i posiada odpowiednie licencje określające właściciela praw autorskich.

Jedynie licencjonowane kopie aplikacji mogą być instalowane w systemie informatycznym Spółki.

Niedopuszczalne jest wykorzystywanie, instalowanie na stacjach roboczych, oprogramowania nieposiadającego licencji oraz jakiekolwiek modyfikacje oprogramowania niezgodne z warunkami licencji. Odpowiedzialność dyscyplinarną i karną w tym zakresie ponosi użytkownik danego stanowiska komputerowego.

Przez szkodliwe oprogramowanie rozumieć należy takie, które:

- ma zdolność samopowielania i/lub samoinstalacji;
- ma zdolność uszkadzania lub modyfikacji pamięci komputerowej, plików systemowych lub oprogramowania w sposób utrudniający wykorzystanie systemów informatycznych;
- służy do omijania lub przełamywania zabezpieczeń i/lub praw dostępu;
- wymusza wykorzystanie większej ilości zasobów informatycznych, niż jest to niezbędne do zapewnienia prawidłowego działania systemów informatycznych Spółki;
- powodowałoby zakłócenia w działaniu sieci informatycznej Spółki;
- powodowałoby naruszenie zasad integralności, rozliczalności, dostępności i poufności przetwarzanych danych osobowych.

Zabronione jest opracowywanie, generowanie, kompilowanie, kopiowanie, rozpowszechnianie, uruchamianie lub próby wprowadzania kodów komputerowych oprogramowania spełniającego powyższe warunki.

10.8.1. AKTUALIZACJA OPROGRAMOWANIA

W celu zapewnienia odpowiedniego poziomu bezpieczeństwa systemu informatycznego, aplikacje służące do bieżącego przetwarzania zasobów informacyjnych Spółki muszą być bieżąco monitorowane pod kątem dostępności nowych wersji, poprawek lub aktualizacji.

Podstawową techniką realizacji wymagań związanych z aktualizacją oprogramowania jest korzystanie z funkcji ich automatycznego pobierania i instalowania. W przypadku braku takiej możliwości, szczególnie w systemach niepodłączonych do sieci Internet, należy możliwie regularnie śledzić informacje udostępniane przez producenta oprogramowania i dokonywać „ręcznej" jego aktualizacji.

Za aktualizację oprogramowania odpowiada ASI.

10.8.2. OPROGRAMOWANIE ANTYWIRUSOWE

Wszystkie elementy systemu informatycznego, tj. serwery, stacje robocze, należy wyposażyć w oprogramowanie antywirusowe sprawujące ciągły nadzór nad pracą systemu i jego zasobami, tzw. „praca w tle". Oprogramowanie antywirusowe powinno być skonfigurowane w sposób uniemożliwiający ingerencję użytkowników stacji roboczych.

Do obowiązków ASI należy aktualizacja oprogramowania antywirusowego oraz określenie częstotliwości automatycznych aktualizacji definicji wirusów dokonywanych przez to oprogramowanie.

Zaleca się używanie innego oprogramowania antywirusowego w stosunku do serwerów i stacji roboczych.

Dobór środków ochrony przed szkodliwym oprogramowaniem powinien być realizowany stosownie do pojawienia się nowych zagrożeń, a także do rozbudowy systemu informatycznego i powiększania baz danych.

10.8.3. ZABEZPIECZENIA FIZYCZNE

W przypadku stacji roboczych, na których przetwarzane są zbiory danych osobowych, zalecane jest blokowanie komunikacji bezprzewodowej (np. WiFi czy Bluetooth).

10.9. ZABEZPIECZENIA KRYPTOGRAFICZNE

Wszelkie dane osobowe przetwarzane w formie elektronicznej przez Spółkę przekazywane poza pomieszczenia Spółki muszą być chronione metodami kryptograficznymi. Za przekazywanie poza

pomieszczenia Spółki należy uznawać informacje wysyłane pocztą elektroniczną oraz przekazywane na komputerowych nośnikach informacji.

Mając na uwadze łatwość stosowania, a przede wszystkim skuteczność zapewnienia informacjom poufności i integralności, należy korzystać z metody szyfrowania.

Za zabezpieczenia kryptograficzne stosowane w Spółce odpowiedzialny jest ASI.

10.9.1. METODY SZYFROWANIA

Szyfrowanie danych należy stosować w sposób i przy użyciu rozwiązań określonych przez ASI. Dobór rozwiązań szyfrujących powinien być dostosowany do charakteru przesyłanych danych osobowych, okresu, przez jaki informacje mają być przechowywane w sposób zapewniający ich poufność i zmieniających się warunków technologicznych.

Szczególnie w sytuacji przesyłania zaszyfrowanych danych do odbiorców spoza Spółki należy pamiętać o stosowaniu międzynarodowych standardów szyfrowania.

10.9.2. KLUCZE SZYFRUJĄCE

Klucze szyfrujące (lub hasła) i zaszyfrowane dane osobowe przesyła się różnymi kanałami telekomunikacyjnymi.

W przypadku przechowywania zaszyfrowanych danych osobowych na nośnikach, nie należy przechowywać na tym samym nośniku kluczy szyfrujących (lub haseł) i związanych z nimi materiałów w postaci niezaszyfrowanej.

Stosowane metody generowania kluczy szyfrujących (lub haseł) muszą być odpowiednio trudne do odtworzenia. Wszystkie klucze szyfrujące (lub hasła) muszą mieć zdefiniowany okres ich ważności. Zmiana musi nastąpić najpóźniej w terminie upływu jego ważności. Nowy klucz (lub hasło) należy wygenerować ze stosowanym wyprzedzeniem i przetestować. Przez cały okres ważności informacji zaszyfrowanej z użyciem klucza szyfrującego (lub hasła) musi on być przechowywany i zabezpieczony przed dostępem osób nieupoważnionych.

10.9.3. PODPIS ELEKTRONICZNY

Dla celów jednoznacznej identyfikacji nadawców i autentyczności dokumentów elektronicznych zaleca się stosowanie certyfikowanego podpisu elektronicznego określonego w Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. 2016 poz. 1579 z późn. zm.).

Zasady korzystania z certyfikowanego podpisu elektronicznego określone są przez dostawców usługi.

10.10. BEZPIECZEŃSTWO ZASOBÓW SPRZĘTOWYCH

10.10.1. WPROWADZANIE URZĄDZEŃ DO UŻYTKU

Należy bezwzględnie zapewnić, aby wszelkie nowe urządzenia komputerowe, platformy, systemy i aplikacje były zgodne z już wykorzystywanymi, a tym samym nie powodowały obniżenia poziomu bezpieczeństwa zasobów informacyjnych. Za wybór sprzętu i jego autoryzację odpowiedzialny jest ASI.

Wszelki zakupiony sprzęt komputerowy przed włączeniem do systemu informatycznego musi obowiązkowo przejść procedurę testowania pod kątem sprawności, funkcjonalności i bezpieczeństwa. Niedopuszczalne jest wprowadzanie do systemu informatycznego sprzętu niespełniającego wymagań określonych Polityce oraz aktach prawnych.

10.10.2. ZABEZPIECZENIE PRZED CZYNNIKAMI ŚRODOWISKOWYMI

W celu ochrony wrażliwych na oddziaływanie szkodliwych czynników środowiskowych elementów systemu informatycznego należy podejmować niezbędne działania w celu ograniczenia lub minimalizacji ich skutków. Należy monitorować czynniki środowiskowe takie jak temperatura, wilgotność, zapylenie w celu identyfikacji sytuacji mogących mieć negatywny wpływ na działanie urządzeń komputerowych. Zasada ta dotyczy w szczególności pomieszczeń, w których znajduje się sprzęt o kluczowym znaczeniu dla bezpieczeństwa informatycznego.

10.11. PRZEGLĄDY, KONSERWACJA I NAPRAWA SPRZĘTU KOMPUTEROWEGO

10.11.1. OKRESOWE PRZEGLĄDY I KONSERWACJA

W celu zapewnienia odpowiedniej poufności, dostępności i integralności informacji przetwarzanych w systemie informatycznym należy poddawać systematycznym przeglądom i konserwacji urządzenia komputerowe. Przeglądy i konserwacje należy wykonywać doraźnie, jednak nie rzadziej niż jest to określone przez dostawców sprzętu.

Przegląd i konserwację systemu wykonują:

- ASI w ramach bieżącej konserwacji,
- podmioty zewnętrzne uprawnione przez ADO do wykonywania naprawy i konserwacji, w obszarze przetwarzania danych osobowych, na podstawie zawartej umowy,

- podmioty zewnętrzne, nieuprawnione do dostępu do systemu, w ramach usług serwisowych, na podstawie zawartej umowy.

Wykaz podmiotów zewnętrznych prowadzi ASI. Czynności wykonywane przez zewnętrznych serwisantów muszą być ściśle nadzorowane przez ASI i w miarę możliwości prowadzone w pomieszczeniach Spółki.

10.11.2. NAPRAWY

Wszystkie awarie (podejrzenia awarii), naprawy oraz działania prewencyjne muszą być bezwzględnie rejestrowane w celu zbierania informacji pozwalających na należyte planowanie zmian w systemie informatycznym oraz opracowywanie działań zaradczych. Za prowadzenie rejestru awarii i napraw odpowiedzialny jest ASI.

O każdym przypadku awarii i naprawy urządzeń systemu informatycznego, w którym przetwarzane są informacje prawnie chronione należy powiadomić osobę wyznaczoną do nadzoru nad ich bezpieczeństwem.

W przypadku konieczności realizacji naprawy urządzeń systemu informatycznego poza siedzibą Spółki, należy bezwzględnie usunąć wszelkie nośniki danych z uszkodzonych urządzeń lub w inny sposób trwale usunąć zasoby informacyjne.

Niedopuszczalne jest przekazywanie do naprawy sprzętu zawierającego bazy danych osobowych.

10.12. WYCOFYWANIE Z UŻYCIA I UTYLIZACJA SPRZĘTU KOMPUTEROWEGO

10.12.1. WYMIANA SPRZĘTU

Decyzję o konieczności wymiany elementów systemu informatycznego podejmuje ASI. Częstotliwość wymiany sprzętu komputerowego określa jego funkcjonalność, przy uwzględnieniu zaleceń producenta.

Urządzenia systemu informatycznego, w szczególności zawierające nośniki danych, należy bezwzględnie poddać sprawdzeniu pod kątem ich zawartości, zainstalowanych aplikacji, szkodliwego oprogramowania. W przypadku stwierdzenia nieautoryzowanych baz danych, nieuprawnionych zasobów informacyjnych, plików zawierających zakazane prawnie informacje, itp., należy o tym fakcie niezwłocznie powiadomić ADO.

Wszystkie wycofane z użytku urządzenia systemu informatycznego należy pozbawić nośników danych, a te, na których nie stwierdzono nieuprawnionych informacji należy sformatować narzędziami systemowymi.

10.12.2. PRZECHOWYWANIE I ZBYCIE SPRZĘTU WYCOFANEGO Z UŻYTKU

Sprzedaż zbędnego sprzętu komputerowego wycofanego z użycia w systemie informatycznym może nastąpić wyłącznie za zgodą ADO.

Sprzęt komputerowy przeznaczony do zbycia może być przekazany dopiero po trwałym usunięciu nośników informacji. Obowiązku fizycznego usunięcia nośników informacji ze sprzętu przeznaczonego do sprzedaży nie można w żadnym wypadku zastąpić jakimkolwiek procesem kasowania danych. Wycofany z użycia sprzęt elektroniczny utylizowany jest na zasadach ogólnych dla zużytego sprzętu elektronicznego.

Wszelkie nośniki informacji wykorzystywane w systemie informatycznym po ustaniu ich przydatności podlegają obowiązkowej utylizacji. Proces utylizacji ma za zadanie trwałe zniszczenie nośników, uniemożliwiające odczytanie zawartych w nich informacji, mając na uwadze obecny stan techniki. Nośniki i urządzenia zawierające dane osobowe przekazywane właściwym podmiotom w celu utylizacji następują po wcześniejszym zawarciu umowy o przetwarzanie danych osobowych lub trwałym usunięciu danych.

Za utylizację nośników informacji odpowiedzialny jest ASI.

11. ZGŁASZANIE INCYDENTÓW

Każdy pracownik Spółki, a także osoby „z zewnątrz" posiadające upoważnienia dostępu do danych osobowych, zobowiązany jest do informowania ASI o wszelkich zauważonych lub podejrzanych słabościach procesu przetwarzania danych osobowych, a w szczególności o:

- naruszeniu hasła i identyfikatora, uprawniających do pracy w systemie informatycznym, np. system nie reaguje na hasło lub je ignoruje, można przetwarzać dane bez wprowadzania hasła;
- częściowym lub całkowitym braku danych albo dostępie do danych w zakresie szerszym niż wynikający z przyznanych uprawnień;
- braku dostępu do właściwej aplikacji lub zmianie zakresu wyznaczonego dostępu do zasobów serwera;
- wykryciu wirusa komputerowego;
- zauważaniu próby włamania do systemu informatycznego;
- znacznym spowolnieniu działania systemu informatycznego;
- podejrzeniu kradzieży sprzętu komputerowego lub dokumentów zawierających dane osobowe;
- zmianie położenia sprzętu komputerowego;
- zauważeniu śladów usiłowania lub dokonania włamania do pomieszczeń lub zamykanych szaf.

11.1. CZYNNOŚCI WSTĘPNE

Do czasu przybycia na miejsce ASI należy:

- podjąć czynności niezbędne do powstrzymania niepożądanych skutków zaistniałego zdarzenia, a następnie uwzględnić w działaniu również ustalenie jego przyczyn lub sprawców;
- rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia;
- zaniechać dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę;
- zastosować się do instrukcji i regulaminów lub dokumentacji aplikacji, jeśli odnoszą się do zaistniałego przypadku;
- przygotować opis incydentu;
- nie opuszczać bez uzasadnionej przyczyny miejsca zdarzenia.

11.2. DZIAŁANIA WYJAŚNIAJĄCE I NAPRAWCZE

ASI po otrzymaniu zawiadomienia o zaistniałym incydencie:

- niezwłocznie przeprowadza postępowanie wyjaśniające, w celu ustalenia okoliczności naruszenia ochrony danych osobowych;
- niezwłocznie podejmuje działanie chroniące system przed ponownym naruszeniem;
- w przypadku stwierdzenia faktycznego naruszenia bezpieczeństwa zasobów informacyjnych Spółki sporządza raport opisujący naruszenie.

ASI w razie potrzeby, może zarządzić odłączenie części systemu informatycznego Spółki dotkniętego incydentem od pozostałej jego części.

W razie odtwarzania danych z kopii zapasowych ASI obowiązany jest upewnić się, że odtwarzane dane zapisane zostały przed wystąpieniem incydentu. Dotyczy to zwłaszcza przypadków infekcji wirusowej.

ADO po zapoznaniu się ze sporządzonym przez ASI raportem dotyczącym naruszenia bezpieczeństwa danych osobowych, podejmuje decyzję o dalszym trybie postępowania, powiadomieniu właściwych organów oraz podjęciu innych, szczególnych czynności zapewniających bezpieczeństwo bądź zastosowaniu środków ochrony fizycznej.

11.3. ZGŁOSZENIA NARUSZENIA OCHRONY DANYCH OSOBOWYCH DO ORGANU NADZORCZEGO

Naruszenie 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. W przypadku naruszenia ochrony danych osobowych, ADO bez zbędnej zwłoki –w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

Zgłoszenie 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 danych osobowych, których dotyczy naruszenie;
- zawierać dane 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.

Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, należy je udzielać sukcesywnie bez zbędnej zwłoki.

Wzór zgłoszenia naruszenia danych stanowi załącznik nr 8 do niniejszej Polityki.

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

Zawiadomienie osoby jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz przynajmniej:

- zawiera dane punktu kontaktowego, od którego można uzyskać więcej informacji;
- opisuje możliwe konsekwencje naruszenia ochrony danych osobowych;

- opisuje 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.

Zawiadomienie osoby nie jest wymagane, w następujących przypadkach:

- ADO wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
- ADO zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
- wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

Przykładowo zawiadomienie osoby jest wymagane w przypadkach:

- kradzieży sprzętu komputerowego zawierającego dane osobowe,
- bezprawnego dostępu do danych osobowych wskutek podatności systemu/aplikacji na ataki sieciowe.

11.4. MONITORING INCYDENTÓW

ADO dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. ADO zobowiązany jest do prowadzenia rejestru zliczającego i monitorującego rodzaj, rozmiar i koszty zaistniałych incydentów. Informacje te należy wykorzystywać do identyfikacji powtarzających się zdarzeń i przypadków niewłaściwego funkcjonowania procesu przetwarzania danych osobowych. Zebrane informacje należy analizować pod kątem potrzeb rozszerzenia istniejących lub wdrożenia dodatkowych zabezpieczeń sytemu informatycznego w celu zmniejszenia częstotliwości i/lub skutków występowania takich zdarzeń w przyszłości.

Wzór rejestru naruszeń stanowi załącznik nr 9 do niniejszej Polityki.

12. PRAWA OSÓB, KTÓRYCH DANE OSOBOWE SĄ PRZETWARZANE

12.1. PRAWO DO INFORMACJI

ADO ma obowiązek informować osobę o przetwarzaniu jej danych w sytuacjach:

- zbierając dane bezpośrednio od tej osoby (art. 13 RODO),
- zbierając dane o osobie z innych źródeł niż ta osoba (art. 14 RODO),
- zmieniając cel przetwarzania danych lub dodając nowy (art. 13 ust. 3 i art. 14 ust. 4 RODO),
- w wykonaniu żądania dostępu do danych (art.15 RODO).

ADO ma obowiązek informowania:

- w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca – mając na uwadze konkretne okoliczności przetwarzania danych osobowych;
- jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą;
- jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.

W celu zrealizowania obowiązku informowania osoby, której dane są przetwarzane ADO:

- umieszcza na stronie internetowej w łatwo dostępnym, widocznym miejscu informacje na temat Polityki prywatności obowiązującej w Spółce.
- wręcza za pokwitowaniem nowemu pracownikowi/osobie zatrudnionej na podstawie umowy cywilnoprawnej pisemną informację o treści wskazane w załączniku nr 3 w chwili podpisywania umowy;

12.1.1. DANE ZBIERANE OD OSOBY, KTÓREJ DANE DOTYCZĄ

ADO przekazuje w zwięzłej, przejrzystej, zrozumiałej oraz łatwo dostępnej formie, a także jasnym i prostym językiem, w tym w formie graficznej, następujące informacje:

- swoją tożsamość i dane kontaktowe,
- cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania, tj. art. 6 ust. 1 lit a), b), c) RODO;
- jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) RODO – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;
- informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją,
- gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz warunkach tego przekazania;

- okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
- informacje o przysługujących osobie, której dane dotyczą prawach;
- jeżeli przetwarzanie odbywa się na podstawie zgody, informacje o prawie do jej cofnięcia w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na jej podstawie przed jej cofnięciem;
- informacje o prawie wniesienia skargi do organu nadzorczego;
- informacje, 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;
- informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu;

12.1.2. DANE ZBIERANE NIE OD OSOBY, KTÓREJ DANE DOTYCZĄ

W przypadkach, gdy Spółka wejdzie w posiadanie danych nie od osoby, które jej dotyczą, oprócz informacji wskazanych w pkt 12.1.1. Polityki podaje się dodatkowo informacje o:

- kategoriach danych, które pozyskano,
- źródło danych, w tym wyszczególnienie źródeł publicznie dostępnych, jeśli z nich skorzystano.

12.2. PRAWO DOSTĘPU DO DANYCH

Osoba, której dane dotyczą, jest uprawniona do uzyskania od ADO 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;
- informacje o prawie do żądania od ADO sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
- informacje o prawie wniesienia skargi do organu nadzorczego;

- jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle.

ADO bez żadnej opłaty dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, Administrator może pobrać rozsądną opłatę. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się bezpłatnie powszechnie stosowaną drogą elektroniczną.
Przed udostępnieniem żądanych informacji, w szczególności zaś przed udzieleniem dostępu do danych osobowych lub wydaniu kopii danych osobowych, w tym elektronicznie, uprawniony pracownik Spółki weryfikuje tożsamość osoby, zgłaszającej żądanie.

12.3. PRAWO SPROSTOWANIA I UZUPEŁNIENIA DANYCH

Pracownik, osoba współpracująca na podstawie umowy cywilnoprawnej, mają prawo zażądać w każdym momencie niezwłocznego sprostowania danych osobowych ich dotyczących. Wskazane osoby mają również prawo żądania uzupełnienia niekompletnych danych osobowych na swój temat, w tym poprzez przedstawienie dodatkowego oświadczenia.

ADO informuje o sprostowaniu danych osobowych każdego Odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. ADO informuje osobę, której dane dotyczą, o tych Odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

12.4. PRAWO DO USUNIĘCIA DANYCH (BYCIA ZAPOMNIANYM)

Spółka odmawia zrealizowania żądania pracownika do usunięcia danych (bycia zapomnianym) w odniesieniu do danych osobowych zawartych w dokumentacji pracowniczej przez cały wymagany przepisami prawa okres archiwizacji dokumentacji określony w pkt. 13 Polityki.

Spółka odmawia zrealizowania żądania osoby współpracującej na podstawie umowy cywilnoprawnej do usunięcia danych (bycia zapomnianym) przez cały wymagany przepisami prawa okres archiwizacji dokumentacji określony w pkt. 13 Polityki.

Spółka realizuje prawo kontrahenta, pracownika i osoby współpracującej na innej podstawie do bycia zapomnianym po upływie okresów retencji dokumentów wskazanych w pkt. 13 Polityki w sytuacji, gdy:

- dane nie są już dłużej niezbędne do realizacji celu, w jakim zostały zebrane lub są przetwarzane;

- podmiot danych wycofał zgodę na przetwarzanie jego danych osobowych oraz nie istnieją podstawy prawne, aby mimo tego kontynuować przetwarzanie;
- podmiot danych sprzeciwia się przetwarzaniu oraz nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania.

12.5. PRAWO DO ŻĄDANIA OGRANICZENIA PRZETWARZANIA DANYCH

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

- osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający ADO 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.

Jeżeli przetwarzanie zostało ograniczone, takie dane osobowe można przetwarzać, z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.

ADO informuje o ograniczeniu przetwarzania każdego Odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. ADO informuje osobę, której dane dotyczą, o tych Odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

12.6. PRAWO DO PRZENOSZENIA DANYCH

Kontrahent, pracownik, osoba współpracująca na podstawie umowy cywilnoprawnej nie mają prawa do żądania przenoszenia danych z uwagi na fakt, że dane ich dotyczące nie są przetwarzane wyłącznie w sposób zautomatyzowany i na podstawie wyrażonej przez nich zgody.

W przypadku otrzymania żądania związanego z wykonywaniem prawa do przenoszenia danych, Spółka informuje o braku podstawy prawnej tego prawa oraz informuje o trybie w jakim możliwe jest uzyskanie dostępu do danych.

12.7. PRAWO DO SPRZECIWU

Prawo do sprzeciwu wobec przetwarzania danych osobowych znajduje zastosowanie tylko i wyłącznie wobec danych osobowych przetwarzanych przez Spółkę w oparciu o przesłankę tzw. prawnie uzasadnionych interesów Spółki jako ADO (art. 6 ust. 1 lit. f RODO).

W innych przypadkach w sytuacji otrzymania żądania związanego z wykonywaniem prawa do sprzeciwu Spółka informuje o braku podstawy prawnej realizacji tego prawa.

12.8. CZAS REALIZACJI PRAW

W ciągu miesiąca od dnia otrzymania wniosku o realizację praw określonych w pkt. 12.1-12.7 Polityki należy udzielić osobie zwrotnej odpowiedzi o:

- nieprzetwarzaniu jej danych albo
- odmowie rozpoznania wniosku (wraz z informacją o prawie do skargi i do sądu), albo
- spełnieniu wniosku, albo
- przedłużeniu działań o (maksymalnie) dwa miesiące ze względu na skomplikowany charakter żądania lub ich liczbę.

12.9. POTWIERDZANIE TOŻSAMOŚCI

Spółka jest zobowiązana do weryfikacji tożsamości przed spełnieniem obowiązków informacyjnych lub udzieleniem odpowiedzi na żądania wynikające z przepisów RODO określone w pkt. 12 Polityki.

13. RETENCJA DANYCH OSOBOWYCH

Listy płac, karty wynagrodzeń oraz inne dokumenty, na podstawie których następuje ustalenie podstawy wymiaru emerytury lub renty, przechowuje się przez okres 50 lat od dnia zakończenia przez ubezpieczonego pracy u danego płatnika (art. 125a ust. 4 ustawy o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (tekst jednolity: Dz.U. 2017 poz. 1383)).

Jednakże dokumenty te przechowuje się przez okres 10 lat od końca roku kalendarzowego, w którym:

- ubezpieczony zakończył pracę u danego płatnika składek, w przypadku ubezpieczonego zgłoszonego u danego płatnika składek do ubezpieczeń po dniu 31 grudnia 2018 r.;
- został złożony raport informacyjny, o którym mowa w art. 4 pkt 6a ustawy z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych w przypadku pracowników zatrudnionych w okresie po dniu 31.12.1998, a przed 01.01.2019.

Akta osobowe:

- pracowników przechowywane są 50 lat od dnia zakończenia pracy u danego pracodawcy (art. 51u ustawy o narodowym zasobie archiwalnym i archiwach z dnia 14 lipca 1983 r).
- pracowników zatrudnionych od 01.01.2019 r przechowuje się 10 lat (art 94 pkt 9b Kodeksu pracy).

Ewidencja czasu pracy pracowników podlegających ogólnym, kodeksowym przepisom prawa:

- przechowywana jest 3 lata od zakończenia okresu, którego dotyczy z uwagi na 3-letni okres przedawnienia roszczeń ze stosunku pracy (art. 291 § 1 Kodeksu pracy z dnia 26 czerwca 1974 r.);
- Umowy cywilnoprawne – do czasu upływu terminów przedawnienia wynikających z nich roszczeń, umowa o dzieło – 2 lata od dnia oddania dzieła (art. 646 Kodeksu cywilnego), pozostałe umowy - 6 lat, a dla roszczeń o świadczenia okresowe oraz roszczeń związanych z prowadzeniem działalności gospodarczej – 3 lata. Koniec terminu przedawnienia przypada na ostatni dzień roku kalendarzowego, chyba że termin przedawnienia jest krótszy niż dwa lata (art. 118 Kodeksu cywilnego);
- dokumenty księgowe niezbędne do rozliczeń przed Urzędem Skarbowym przechowywane są przez 5 lat od zakończenia roku, w którym zaktualizował się obowiązek podatkowy (art. 32 w zw. art. 70 § 1 Ordynacji podatkowej z dnia 20 sierpnia 1997 r.).

ZUS - dokumenty rozliczeniowe, tj. ZUS RCA, ZUS RZA, ZUS RSA, ZUS DRA - kopie deklaracji rozliczeniowych i imiennych raportów miesięcznych oraz dokumentów korygujących te dokumenty płatnik składek jest zobowiązany przechowywać przez okres 5 lat od dnia ich przekazania do wskazanej przez Zakład jednostki organizacyjnej Zakładu, w formie dokumentu pisemnego lub elektronicznego (art. 47 ust. 3c ustawy o systemie ubezpieczeń społecznych).

Rejestr wypadków przy pracy - istnieje w sposób ciągły, jednakże protokół powypadkowy przechowuje się przez 10 lat (art. 234§3^1 Kodeksu Pracy):

- dokumentacja związana z wypadkami zbiorowymi, śmiertelnymi i powodującymi inwalidztwo - przechowuje się 25 lat.
- Statystyczna karta wypadków - sporządzana w 2 egzemplarzach (jeden dla urzędu statystycznego, drugi egzemplarz pracodawca przechowuje 10 lat).

14. POWIERZENIE DANYCH DO PRZETWARZANIA PODMIOTOWI ZEWNĘTRZNEMU

ADO może powierzyć innemu podmiotowi – Przetwarzającemu - przetwarzanie danych osobowych, jeżeli jest to uzasadnione potrzebami Spółki lub wynika z obowiązku prawnego. Powierzenie danych osobowych do przetwarzania podmiotowi zewnętrznemu może nastąpić wyłącznie w drodze umowy zawartej na piśmie. ADO przed zawarciem umowy powierzenia danych osobowych do przetwarzania podmiotowi zewnętrznemu zobowiązany jest do potwierdzenia czy spełnia on wymogi w zakresie zabezpieczeń organizacyjno-technicznych oraz dokumentacji procesu przetwarzania danych osobowych. Ponadto Przetwarzający musi mieć ustanowionego Inspektora Ochrony Danych Osobowych w przypadku powierzenia mu do przetwarzania Szczególnych kategorii danych osobowych w dużej ilości.

Za czynność powierzenia danych osobowych do przetwarzania przyjmuje się także zawarcie z podmiotem zewnętrznym umowy na zarządzanie i serwis systemu informatycznego, archiwizowanie dokumentacji tradycyjnej, niszczenie nośników danych osobowych (tradycyjnych i informatycznych), itp.

Powierzenie danych osobowych do przetwarzania podmiotowi zewnętrznemu nie zdejmuje z ADO odpowiedzialności za ich bezpieczeństwo.

14.1. UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

Umowa powierzenia przetwarzania danych osobowych powinna zawierać w szczególności:

- ogólne oświadczenie opisujące stanowisko Spółki w zakresie bezpieczeństwa danych osobowych;
- oświadczenie Przetwarzającego, iż spełnia on wymagania w zakresie bezpieczeństwa danych,
- zobowiązanie Przetwarzającego do przestrzegania adekwatnych środków ochrony, wymaganych na mocy art. 32 RODO,
- oświadczenie Przetwarzającego, że przetwarza dane osobowe wyłącznie na udokumentowane polecenie ADO,
- określenie celu i zakresu przetwarzania powierzonych danych osobowych;
- określenie rodzaju danych osobowych oraz kategorii osób, których dotyczą,
- określenie sposobu wypełniania wymagań prawnych związanych z przetwarzaniem danych osobowych
- wymóg uzyskania pisemnej zgody od ADO na korzystanie przez Przetwarzającego z usług innego podmiotu przetwarzającego lub klauzulę zgody ogólnej z obowiązkiem informowania ADO o wybranym podmiocie i możliwości wyrażenia przez ADO sprzeciwu co do tego wyboru;

- zobowiązanie do dokumentowania przetwarzania danych, w tym prowadzenia rejestru kategorii czynności przetwarzania danych osobowych,
- prawo ADO do przeprowadzania lub zlecania kontroli sposobu realizacji postanowień umowy, ze szczególnym uwzględnieniem zapewnienia wymaganego poziomu bezpieczeństwa przetwarzanych danych osobowych;
- zapewnienie o współpracy z ADO w odpowiadaniu na żądania osób, których dane dotyczą oraz w wykonywaniu obowiązków określonych w art. 32 – 36 RODO, tj. zachowaniu bezpieczeństwa poprzez wdrożenie odpowiednich środków technicznych, współdziałanie przy stwierdzonych naruszeniach ochrony danych osobowych (zobowiązanie do przekazywania informacji w ciągu max. 24 godzin) oraz przy tworzeniu oceny skutków przetwarzania danych,
- klauzule poufności w zakresie zachowania tajemnicy lub zapewnienie, że osoby przetwarzające dane osobowe podlegają odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
- zobowiązania Przetwarzającego i jego podwykonawców do nieprzetwarzania danych poza Europejskim Obszarem Gospodarczym oraz o poinformowaniu ADO o takim zamiarze;
- zobowiązanie do usuwania i zwrotu po zakończeniu umowy danych i ich kopii;
- zakaz podzlecenia świadczenia głównego;
- kary umowne za nieprzestrzeganie zapisów umowy.

Zapisy dotyczące powierzenia danych osobowych do przetwarzania mogą stanowić odrębną umowę lub stanowić integralną część umowy dotyczącej konkretnej usługi lub zlecenia. Wzór umowy powierzenia przetwarzania danych osobowych stanowi załącznik nr 10 do niniejszej Polityki

14.2. PRZETWARZANIE DANYCH PRZYJĘTYCH DO PRZETWARZANIA OD PODMIOTU ZEWNĘTRZNEGO

W stosunku do danych osobowych przyjętych do przetwarzania od podmiotu zewnętrznego ADO pełnił będzie funkcję Przetwarzającego. Dalsze powierzenie danych osobowych przyjętych do przetwarzania od podmiotu zewnętrznego powinno następować zgodnie z postanowieniami umowy z podmiotem zewnętrznym. W przypadku przetwarzania danych przyjętych od podmiotu zewnętrznego Spółka prowadzi rejestr kategorii czynności przetwarzania, którego wzór stanowi załącznik nr 11 do niniejszej Polityki.

15. PROJEKTOWANIE PRYWATNOŚCI

Wszelkie procedury uruchamiania nowych projektów i inwestycji w Spółce uwzględniają konieczność oceny wpływu zmiany na ochronę danych, analizę ryzyka, zapewnienie prywatności (a w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany, inwestycji lub na początku nowego projektu.

16. REJESTR CZYNNOŚCI PRZETWARZANIA

ADO opracowuje, prowadzi i utrzymuje Rejestr Czynności Przetwarzania Danych Osobowych w Spółce (Rejestr). Rejestr jest zasadniczym narzędziem monitorowania i rozliczania Spółki z realizacji obowiązków w zakresie ochrony danych.

W Rejestrze dla każdej czynności przetwarzania danych, którą Spółka uznała za odrębną dla potrzeb Rejestru, odnotowuje się co najmniej:

- nazwę czynności,
- cel przetwarzania,
- opis kategorii osób,
- opis kategorii danych,
- podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu, jeśli podstawą jest uzasadniony interes,
- sposób zbierania danych,
- opis kategorii odbiorców danych (w tym przetwarzających),
- informację o przekazaniu poza EU/EOG;
- ogólny opis technicznych i organizacyjnych środków ochrony danych - jeżeli jest to możliwe.

Wzór rejestru czynności przetwarzania stanowi załącznik nr 12 do niniejszej Polityki.

17. AKTUALIZACJA DOKUMENTACJI OCHRONY DANYCH OSOBOWYCH

ADO, bądź wyznaczona przez niego osoba, przeprowadza raz w roku przegląd przetwarzanych danych osobowych pod kątem celowości ich dalszego przetwarzania.

Osoby upoważnione do przetwarzania danych osobowych są zobowiązane do:

- współpracy w tym zakresie z wyznaczoną osobą;
- udzielania niezbędnych informacji.

ADO może zarządzić przeprowadzenie dodatkowego przeglądu w wyżej określonym zakresie w razie zmian w obowiązującym prawie, ograniczających dopuszczalny zakres przetwarzania danych osobowych. Dodatkowy przegląd może być konieczny także w sytuacji zmian organizacyjnych ADO.

Aktualizacji niniejszej Polityki dokonuje osoba upoważniona przez ADO, a następnie przedkłada ją ADO celem zatwierdzenia zmian.

18. AUDYT PROCESU PRZETWARZANIA DANYCH OSOBOWYCH

Utrzymanie bezpieczeństwa danych osobowych na wysokim, akceptowalnym poziomie, spełniającym w tym zakresie obowiązki wynikające z prawa powszechnie obowiązującego wymaga systematycznej analizy aktualności procedur bezpieczeństwa oraz stopnia ich przestrzegania.

Audyt jest podstawową i kompleksową formą dokonania analizy, systematyzacji i oceny istniejącego stanu ochrony danych osobowych przetwarzanych w Spółce. Profesjonalnie i rzetelnie przeprowadzony audyt bezpieczeństwa danych osobowych pozwala przygotować raport przedstawiający przede wszystkim stan faktyczny zasobów informacyjnych i ich bezpieczeństwa oraz działania, które pozwolą dostosować Spółkę do aktualnych potrzeb w tym zakresie.

Polityka bezpieczeństwa danych osobowych powinna być poddawana przeglądowi przynajmniej raz w roku, by zapewnić jej skuteczność i adekwatność pomimo zachodzących zmian. Ponadto przegląd Polityki należy przeprowadzać w przypadku poważnego naruszenia bezpieczeństwa przetwarzanych danych osobowych, pojawienia się nowych, istotnych rodzajów zagrożeń, zmian regulacji prawnych lub znaczących zmian organizacyjno - technicznych Spółki. ADO wspólnie z ASI zobowiązany jest do cyklicznego przeprowadzania audytów w obszarze wybranych procedur bezpieczeństwa danych osobowych.

ASI zobowiązany jest do systematycznego kontrolowania i testowania bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym Spółki.

Do głównych czynności kontrolnych należą:

- przeglądy pliku zawierającego raport dotyczący działalności aplikacji bądź systemu (logi systemowe), wykonywane nie rzadziej niż raz na miesiąc;
- przeglądy i sprawdzenia poprawności zbiorów danych, wykonywane nie rzadziej niż raz na miesiąc.

Ponadto zapisy logów systemowych powinny być przeglądane przez ASI każdorazowo po wykryciu naruszenia zasad bezpieczeństwa. Kontrole i testy przeprowadzone przez ASI powinny obejmować zarówno dostęp do zasobów systemu, jak i profile oraz uprawnienia poszczególnych użytkowników.

ADO może podjąć decyzję o przeprowadzeniu kompleksowego audytu bezpieczeństwa danych osobowych. Zaleca się aby kompleksowy audyt przeprowadzany były przy udziale niezależnej, wyspecjalizowanej, zewnętrznej instytucji audytorskiej.

Odpowiednio szybka i profesjonalnie przeprowadzona reakcja na zaistniałe zdarzenie, lub podejrzenie zdarzenia, mogącego naruszać bezpieczeństwo zasobów informacyjnych Spółki,

w szczególności prawnie chronionych, daje możliwość właściwej oceny zaistniałej sytuacji i podjęcia niezbędnych działań zmierzających do minimalizacji jej skutków.

Obowiązkiem każdego pracownika Spółki jest zgłaszanie przypadków naruszenia lub groźby naruszenia bezpieczeństwa zasobów informacyjnych Spółki. Zgłaszać należy wszelkie zdarzenia zagrażające lub mogące zagrozić bezpieczeństwu zasobów informacyjnych Spółki. W szczególności incydentami będą wszelkie działania niezgodne z zapisami niniejszej Polityki.

19. „DOBRE PRAKTYKI"

Wszyscy upoważnieni do dostępu do danych osobowych, a w szczególności pracownicy Spółki, zobowiązani są do świadomego posługiwania się narzędziami służącymi do ich przetwarzania, oraz bezwzględnego przestrzegania zasad bezpieczeństwa takich jak:

- kasowanie po wykorzystaniu danych na dyskach przenośnych;
- nieużywanie powtórne jednostronnie zadrukowanych dokumentów zawierających informacje chronione;
- zachowanie poufności, w tym także wobec najbliższych;
- pilne strzeżenie akt, nośników, pamięci przenośnych;
- nie pozostawianie bez kontroli dokumentów, nośników danych i sprzętu w samochodach, hotelach i innych miejscach publicznych;
- ustawianie ekranów komputerowych tak, aby osoby niepowołane nie mogły oglądać wyświetlanych informacji, a zwłaszcza vis-a-vis wejścia do pomieszczenia, w przypadku braku takiej możliwości stosowanie filtrów prywatyzacyjnych oraz zachowanie wzmożonej czujności pracownika wykonującego obowiązki w momencie wejścia do pomieszczenia osób postronnych;
- nie zapisywanie, w żaden sposób, hasła wymaganego do uwierzytelniania się w systemie;
- nie podłączanie do listew podtrzymujących napięcie, przeznaczonych dla sprzętu komputerowego, innych urządzeń, szczególnie tych łatwo powodujących przepięcia, np. grzejniki, wentylatory, czajniki;
- dbanie o prawidłową wentylację komputerów i innych elementów sieci teleinformatycznej;
- powstrzymywanie się od samodzielnej ingerencji w oprogramowanie i konfigurację powierzonego sprzętu (szczególnie komputerów przenośnych), nawet gdy z pozoru mogłoby to usprawnić pracę lub podnieść poziom bezpieczeństwa danych;
- przestrzeganie swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używanie tylko własnego identyfikatora i hasła oraz stosowanie się do zaleceń osób odpowiedzialnych za bezpieczeństwo informacyjne Spółki;

- nie pozostawianie otwartych drzwi do pomieszczeń biurowych w trakcie czasowej nieobecności pracowników;
- nie pozostawianie osób postronnych w pomieszczeniach biurowych, bez nadzoru osoby upoważnionej;
- opuszczanie stanowiska pracy dopiero po aktywacji wygaszacza ekranu lub po zablokowaniu stacji roboczej w inny sposób;
- kopiowanie tylko jednostkowych danych (pojedynczych plików), obowiązuje zakaz robienia kopii całych zbiorów danych lub takich ich części, które nie są konieczne do wykonywania obowiązków przez pracownika;
- udostępnianie danych osobowych w sieci Internet tylko w postaci zaszyfrowanej;
- nie wynoszenie poza obszar przetwarzania na jakichkolwiek nośnikach całych zbiorów danych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej;
- wykonywanie kopii roboczych danych, na których się właśnie pracuje, tak często, aby zapobiec ich utracie;
- kończenie pracy na stacji roboczej po wprowadzeniu danych przetwarzanych tego dnia w odpowiednie obszary serwera, a następnie prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera;
- niszczenie w niszczarce lub chowanie do szaf zamykanych na klucz wszelkich wydruków zawierających informacje chronione, przed opuszczeniem miejsca pracy po zakończeniu dnia pracy;
- chowanie do szaf zamykanych na klucz wszelkich akt zawierających informacje chronione, przed opuszczeniem miejsca pracy po zakończeniu dnia pracy;
- zamykanie okien w razie opadów lub innych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu nośników informacji;
- zamykanie okien w razie opuszczania pomieszczenia, w tym zwłaszcza po zakończeniu dnia pracy;
- sprawdzanie zamknięcia pomieszczeń po zakończeniu pracy w danym dniu.

20. POSTANOWIENIA KOŃCOWE

Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych osobowych z niniejszym dokumentem oraz złożyć stosowne oświadczenie potwierdzające znajomość jego treści.

Polityka wchodzi w życie z dniem ……..

ZAŁĄCZNIK NR 1 – MINIMALNE WYMAGANIA W ZAKRESIE BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Minimalne wymagania w zakresie bezpieczeństwa danych osobowych
A. w zakresie bezpieczeństwa fizycznego
Dokumenty zawierające dane osobowe przechowywane w meblach biurowych zamykanych na klucz.
Pomieszczenia, w których przechowuje się dane osobowe zamykane po zakończeniu pracy.
B. w zakresie bezpieczeństwa osobowego
Upoważnienie do przetwarzania danych osobowych wydane przez ADO.
Zaświadczenie o odbytym szkoleniu z zakresu ochrony danych osobowych prowadzonym przez osobę wyznaczoną przez ADO.
Szkolenie z zakresu obsługi systemu informatycznego prowadzone przez ASI.
Podpisane oświadczenie o zapoznaniu się z przepisami normującymi ochronę danych osobowych.
Podpisane zobowiązanie do zachowania w tajemnicy danych osobowych.
C. w zakresie sprzętu komputerowego i oprogramowania
Odrębny identyfikator dla każdego użytkownika systemu informatycznego.
Hasło użytkownika składające się z minimum 8 znaków zmieniane, co 90 dni, bez możliwości powtórzenia trzech ostatnich haseł.
Automatyczne blokowanie dostępu do nieużywanych urządzeń systemu po 5 minutach bezczynności.
Określona procedura nadawania uprawnień w systemie informatycznym.
Urządzenia systemu zabezpieczone przed kradzieżą.
Urządzenia systemu zabezpieczone przed brakiem zasilania.
Kopie zapasowe zabezpieczone przed nieuprawnionym przejęciem, usuwane niezwłocznie po ustaniu ich aktualności.
Określona procedura tworzenia, przechowywania i użytkowania kopii zapasowych.
Urządzenia przekazywane poza siedzibę Spółki pozbawione nośników zawierających dane osobowe.
Określona procedura postępowania ze sprzętem wymagającym naprawy lub przeznaczonym do likwidacji.
Fizyczne lub logiczne zabezpieczenie systemu informatycznego przed nieautoryzowanym dostępem z sieci Internet.
Zabezpieczenie systemu informatycznego oprogramowaniem antywirusowym.
Określona procedura postępowania w przypadku błędnej pracy systemu informatycznego.
D. w zakresie przekazywania danych osobowych podmiotom zewnętrznym
Zawarta umowa powierzenia przetwarzania danych osobowych.
Ochrona danych osobowych w podmiocie przetwarzającym dane osobowe zapewniona na poziomie, co najmniej takim samym jak w Spółce.
Wykonywanie czynności kontrolnych przez ADO.

ZAŁĄCZNIK NR 2 - WYKAZ I STRUKTURA ZBIORÓW DANYCH OSOBOWYCH

ZBIORY DANYCH OSOBOWYCH ADMINISTRATORA DANYCH			
	ZBIÓR DANYCH	**ZAWARTOŚĆ INFORMACYJNA**	**APLIKACJA**
1.			
2.			
3.			

ZAŁĄCZNIK NR 3 – WZÓR KLAUZULI INFORMACYJNEJ

KLAUZULA INFORMACYJNA

Zgodnie z art. 13 ust. 1 i ust. 2 ogólnego 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 (RODO) z dnia 27 kwietnia 2016 r. informuję, iż:

1. administratorem Pani/Pana danych osobowych jest BezDebetu.pl Sp. z o. o. Sp.k., z siedzibą ul. Powsińska 75 lok. 1, 02-903 Warszawa Wilanów;
2. Pani/Pana dane osobowe przetwarzane są w celu ……. (np. wykonania umowy na podstawie art. 6 ust 1 pkt b RODO);
3. odbiorcą Pani/Pana danych osobowych są pracownicy i podmioty wykonujące usługi na rzecz BezDebetu.pl Sp. z o. o. Sp.k.;
4. Pani/Pana dane osobowe nie będą przekazywane do państwa trzeciego
5. Pani/Pana dane osobowe będą przechowywane przez okres …….. lub do czasu ……. (np. upływu terminów przedawnienia roszczeń wynikających z umów, o których mowa w pkt.2);
6. posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo wniesienia sprzeciwu wobec przetwarzania, prawo do cofnięcia zgody w dowolnym momencie;
7. ma Pani/Pan prawo wniesienia skargi do organu nadzorczego właściwego w sprawach ochrony danych osobowych, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r
8. podanie przez Panią/Pana danych osobowych jest warunkiem …… (np. zawarcia umowy) – o ile dotyczy.

ZAŁĄCZNIK NR 4 – OŚWIADCZENIE O ZACHOWANIU POUFNOŚCI

.....

(imię i nazwisko, stanowisko)

OŚWIADCZENIE

oświadczam, że zapoznałem się z przepisami dotyczącymi ochrony danych osobowych i zobowiązuję się do przestrzegania:

Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119/1 z 04.05.2016);

Ustawy o ochronie danych osobowych z dnia 10 maja 2018 r (Dz.U. z 2018 r. poz. 1000).

„Polityki bezpieczeństwa przetwarzania danych osobowych dla BezDebetu.pl Sp. z o. o. Sp.k.".

Jednocześnie oświadczam, że:

- zapewnię ochronę przetwarzanych przeze mnie danych osobowych, a w szczególności zabezpieczę je przed niedozwolonym lub niezgodnym z prawem przetwarzaniem, przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, uszkodzeniem, modyfikacją, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
- zachowam w tajemnicy, także po ustaniu stosunku pracy, wszelkie informacje dotyczące przetwarzania oraz sposobów zabezpieczania danych osobowych, w tym hasła dostępu do systemu informatycznego,
- natychmiast zgłoszę przełożonemu i ADO stwierdzenie próby lub faktu naruszenia zabezpieczenia pomieszczenia oraz bezpieczeństwa systemu informatycznego, w którym przetwarzane są dane osobowe.

..... Warszawa, dnia .....

(podpis pracownika ubiegającego się o dostęp)

ZAŁĄCZNIK NR 5 – WZÓR POLECENIA PRZETWARZANIA DANYCH OSOBOWYCH

Warszawa, dn. ……

POLECENIE PRZETWARZANIA DANYCH OSOBOWYCH

Zgodnie z art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) polecam

Panu(i): ……
(Imię i Nazwisko)

Zatrudnionemu(ej) na stanowisku ……..
(Nazwa stanowiska)

Przetwarzanie danych osobowych w BezDebetu.pl Sp. z o. o. Sp.k.

w zbiorze pt ”…….”

(pełna nazwa zbioru)

……....

Administrator Danych Osobowych

ZAŁĄCZNIK NR 6 – WZÓR UPOWAŻNIENIA

Warszawa, dn. ……

UPOWAŻNIENIE

Nr …/…./….

do przetwarzania danych osobowych

w BezDebetu.pl Sp. z o. o. Sp.k.

Zgodnie z art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1)

Administrator upoważnia Pana(ią): **……**

(Imię i Nazwisko)

Zatrudnionego(ą) na stanowisku **……**

(Stanowisko)

do przetwarzania danych osobowych w BezDebetu.pl Sp. z o. o. Sp.k.

w zbiorze pt ”…….”

(pełna nazwa zbioru)

Upoważnienie ważne na okres:*

od dnia……do dnia……..*

od dnia……do odwołania*

zatrudnienia*

……..……..……..

Podpis Administratora Danych Osobowych

---

*Niepotrzebne skreślić

ZAŁĄCZNIK NR 7 – WZÓR REJESTRU WYDANYCH UPOWAŻNIEŃ

								Data			System		
lp	nr upoważnienia	login	Nazwisko	Imię	Stanowisko	Oświadczenie o zapoznaniu się z przepisami	Data szkolenia	nadania upoważnienia	ustania upoważnienia	Nazwa Zbioru	Data założenia konta	Data usunięcia konta	Uwagi
1													
2													
3													
4													
5													
6													
7													
8													
9													

ZAŁACZNIK NR 8 – WZÓR ZGŁOSZENIA NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Warszawa, dn. ……

BezDebetu.pl Sp. z o. o. Sp.k.

ul. Powsińska 75 lok. 1

02-903 Warszawa Wilanów

Prezes Urzędu Ochrony Danych Osobowych

Urząd Ochrony Danych Osobowych

ul. Stawki 2

00-193 Warszawa

ZGŁOSZENIE
W SPRAWIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Niniejszym w trybie art. 33 RODO, zgłaszam naruszenie ochrony danych osobowych, które miało miejsce w dniu …… w …….. .

1.	Charakter naruszenia ochrony danych:	
2.	Kategoria i przybliżona liczba osób, których dane dotyczą:	
3.	Liczba rekordów, których dotyczy naruszenie:	
4.	Możliwe konsekwencje naruszenia ochrony danych:	
5.	Środki zastosowane lub proponowane w celu zaradzenia naruszenia ochrony danych osobowych, w tym zastosowane środki w celu zminimalizowania ewentualnych negatywnych skutków naruszenia ochrony danych:	
6.	Dane inspektora ochrony danych	

ZAŁĄCZNIK NR 9 – WZÓR REJESTRU NARUSZEŃ

		1	2	3	4	5
LP.	**Data naruszenia**	**Nazwa/rodzaj naruszenia**	**Okoliczności naruszenia**	**Rozmiar naruszenia**	**Skutki i koszty naruszenia**	**Podjęte działania**
1.						
2.						
3.						
4.						
5.						

ZAŁĄCZNIK NR 10 – WZÓR UMOWY POWIERZENIA

Umowa

powierzenia przetwarzania danych osobowych stanowiąca

uzupełnienie Umowy .....

zawarta w dniu ..... w ..... , między:

..... („**Administrator**")

a

..... („**Przetwarzający**")

(dalej łącznie jako: „**Strony**").

Mając na uwadze, że:

a) Strony zawarły umowę ..... („**Umowa Podstawowa**"), w związku z wykonywaniem której Administrator powierzy Przetwarzającemu przetwarzanie danych osobowych w zakresie określonym Umową;
b) Celem Umowy powierzenie jest ustalenie warunków, na jakich Przetwarzający wykonuje operacje przetwarzania danych osobowych w imieniu Administratora;
c) Strony, zawierając Umowę, dążą do takiego uregulowania zasad przetwarzania danych osobowych, aby odpowiadały one w pełni postanowieniom rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)– dalej **RODO**.

Strony postanowiły zawrzeć Umowę o następującej treści:

1. **Opis przetwarzania**

1.1. **Przedmiot [art. 28 ust. 3 RODO**]. Na warunkach określonych niniejszą Umową oraz Umową Podstawową Administrator powierza Przetwarzającemu przetwarzanie (w rozumieniu RODO) dalej opisanych danych osobowych (dalej w skrócie zwanych też „**danymi**").
1.2. **Czas [art. 28 ust. 3 RODO**]. Przetwarzanie będzie wykonywane w okresie obowiązywania Umowy Podstawowej.
1.3. **Charakter i cel [art. 28 ust. 3 RODO**]. Charakter i cel przetwarzania wynikają z Umowy Podstawowej.

2. **Rodzaj danych [art. 28 ust. 3 RODO**]. Przetwarzanie obejmować będzie następujące rodzaje danych osobowych:

Dane zwykłe:

(1) imię i nazwisko,

(2) numer ewidencyjny PESEL,

(3) adres e-mail,

(4) adres IP,

(5) numery telefonow,

(6) adres zamieszkania,

(7) data urodzenia,

(8) NIP,

(9) seria i numer dokumentu tożsamości,

(10) imiona rodziców,

(11) numer rachunku bankowego,

(12) .....

Dane szczególnych kategorii i dane karne: (o ile dotyczy)

(13) ..... ,

(14) ..... ,

(15) .....

Dane nieustrukturyzowane: (o ile dotyczy)

kontent o potencjalnej i prawdopodobnej zawartości danych osobowych (wpisy, dokumenty tekstowe, obrazy, nagrania, filmy).

3. **Kategorie osób [art. 28 ust. 3 RODO**]. Przetwarzanie danych będzie dotyczyć następujących kategorii osób: klienci usługi/produktu Administratora określonych w Umowie Podstawowej,
4. **Podprocesor**
   - 4.1. **Podprocesor [art. 28 ust. 2 RODO**]. Podmiot przetwarzający może skorzystać z usług innego podmiotu przetwarzającego (Podprocesor) w drodze zawarcia z tym podmiotem pisemnej umowy pod warunkiem, że Administrator udzielił Podmiotowi przetwarzającemu uprzedniej pisemnej, pod rygorem nieważności, zgody (zgoda szczególna w rozumieniu art. 28 ust. 2 RODO) na skorzystanie z usług innego podmiotu przetwarzającego, przy czym za Podprocesora, w rozumieniu Umowy nie uważa się osób fizycznych, którymi posługuje się Podmiot Przetwarzający, niezależnie od formy ich zatrudnienia i za których działania lub zaniechania ponosi odpowiedzialność, z włączeniem osób prowadzących indywidualną działalność gospodarczą.
   - 4.2. **Zaakceptowani Podprocesorzy.** Lista Podprocesorów zaakceptowanych przez Administratora stanowi **Załącznik nr 1 do Umowy – Lista Zaakceptowanych Podprocesorów**.
   - 4.3. **Profesjonalność**. Podmiot przetwarzający korzysta z usług wyłącznie takich Podprocesorów, którzy zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO oraz chroniło prawa osób, których dane dotyczą.
   - 4.4. **Sprzeciw.** Powierzenie przetwarzania danych Podprocesorowi spoza Listy Zaakceptowanych podprocesorów wymaga uprzedniego zgłoszenia Administratorowi w celu umożliwienia wyrażenia sprzeciwu. Administrator może z uzasadnionych przyczyn zgłosić udokumentowany sprzeciw względem powierzenia danych konkretnemu Podprocesorowi. W razie zgłoszenia sprzeciwu Przetwarzający nie ma prawa powierzyć danych Podprocesorowi objętemu sprzeciwem, a jeżeli

sprzeciw dotyczy aktualnego Podprocesora, musi niezwłocznie zakończyć powierzenie temu Podprocesorowi danych. Wątpliwości co do zasadności sprzeciwu i ewentualnych negatywnych konsekwencji Przetwarzający zgłosi Administratorowi w czasie umożliwiającym zapewnienie ciągłości przetwarzania.

4.5. **Transfer obowiązków [art. 28 ust. 4 RODO**]. Dokonując powierzenia Podprocesorowi danych, Przetwarzający ma obowiązek zobowiązać Podprocesora do realizacji wszystkich obowiązków Przetwarzającego wynikających z niniejszej Umowy powierzenia, z wyjątkiem tych, które nie mają zastosowania ze względu na naturę konkretnego powierzenia.

4.6. **Zobowiązanie względem Administratora.** Przetwarzający ma obowiązek zapewnić, aby Podprocesor złożył Administratorowi zobowiązanie do wykonania obowiązków, o których mowa w poprzednim ustępie. Może to zostać wykonane przez podpisanie stosownego oświadczenia adresowanego do Administratora wraz z podpisaniem Umowy, zawierającej listę obowiązków Podprocesora.

4.7. **Zakaz podzlecenia świadczenia głównego [art. 28 ust. 4 RODO**]. Przetwarzający nie ma prawa przekazać Podprocesorowi całości wykonania Umowy.

5. **Obowiązki Przetwarzającego**

5.1. **Udokumentowane polecenia [art. 28 ust. 3 lit. a RODO].** Przetwarzający przetwarza dane wyłącznie zgodnie z udokumentowanymi poleceniami lub instrukcjami Administratora.

5.2. **Nieprzetwarzanie poza EOG [art. 28 ust. 3 lit. a RODO].** Przetwarzający oświadcza, że nie przekazuje danych do państwa trzeciego lub organizacji międzynarodowej (czyli poza Europejski Obszar Gospodarczy – **EOG**). Przetwarzający oświadcza również, że nie korzysta z podwykonawców, którzy przekazują Dane poza EOG.

5.3. **Poinformowanie o zamiarze przetwarzania poza EOG [art. 28 ust. 3 lit. a RODO].** Jeżeli Przetwarzający ma zamiar lub obowiązek przekazywać dane poza EOG, informuje o tym Administratora w celu umożliwienia Administratorowi podjęcia decyzji i działań niezbędnych do zapewnienia zgodności przetwarzania z prawem lub zakończenia powierzenia przetwarzania.

5.4. **Tajemnica [art. 28 ust. 3 lit. b RODO].** Przetwarzający uzyskuje od osób, które zostały upoważnione do przetwarzania danych w wykonaniu Umowy, udokumentowane zobowiązania do zachowania tajemnicy, ewentualnie upewnia się, że te osoby podlegają ustawowemu obowiązkowi zachowania tajemnicy.

5.5. **Bezpieczeństwo [art. 28 ust. 3 lit. c RODO].** Przetwarzający zapewnia ochronę danych i podejmuje środki ochrony danych, o których mowa w art. 32 RODO, zgodnie z dalszymi postanowieniami Umowy.

5.6. **Współpraca przy realizacji praw jednostki [art. 28 ust. 3 lit. e RODO].** Przetwarzający zobowiązuje się wobec Administratora do odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania praw określonych w rozdziale III RODO (tzw..„prawa jednostki"). Przetwarzający oświadcza, że zapewnia obsługę praw jednostki w odniesieniu do powierzonych danych.

5.7. **Wsparcie przy obowiązkach bezpieczeństwa [art. 28 ust. 3 lit. f RODO].** Przetwarzający współpracuje z Administratorem przy wykonywaniu przez Administratora obowiązków z obszaru ochrony danych osobowych, o których mowa w art. 32–36 RODO (ochrona danych, zgłaszanie naruszeń organowi nadzorczemu, zawiadamianie osób dotkniętych naruszeniem ochrony danych, ocena skutków dla ochrony danych i uprzednie konsultacje z organem nadzorczym).

5.8. **Legalność poleceń [art. 28 ust. 3 ak. 2 RODO].** Jeżeli Przetwarzający poweźmie wątpliwości co do zgodności z prawem wydanych przez Administratora poleceń lub instrukcji, Przetwarzający natychmiast informuje Administratora o stwierdzonej wątpliwości (w sposób udokumentowany i z uzasadnieniem), pod rygorem utraty możliwości dochodzenia roszczeń przeciwko Administratorowi z tego tytułu.

5.9. **Projektowanie [art. 25 ust. 1 RODO**]. Planując dokonanie zmian w sposobie przetwarzania danych, Przetwarzający ma obowiązek zastosować się do wymogu projektowania prywatności, o którym mowa w art. 25 ust. 1 RODO, i ma obowiązek z wyprzedzeniem informować Administratora o planowanych zmianach w taki sposób i w takich terminach, aby zapewnić Administratorowi realną możliwość reagowania, jeżeli planowane przez Przetwarzającego zmiany w opinii Administratora grożą uzgodnionemu poziomowi bezpieczeństwa danych lub zwiększają ryzyko naruszenia praw lub wolności osób, wskutek przetwarzania danych przez Przetwarzającego.

5.10. **Minimalizacja [art. 25 ust. 2 RODO**]. Przetwarzający zobowiązuje się do ograniczenia dostępu do danych wyłącznie do osób, których dostęp do danych jest potrzebny do realizacji Umowy i posiadających odpowiednie upoważnienie.

5.11. **RCPD [art. 30 ust. 2 RODO].** Przetwarzający zobowiązuje się do prowadzenia dokumentacji opisującej sposób przetwarzania danych, w tym rejestru czynności przetwarzania danych osobowych (wymóg art. 30 RODO). Przetwarzający udostępniania na żądanie Administratora prowadzony rejestr czynności przetwarzania danych przetwarzającego, z wyłączeniem informacji stanowiących tajemnicę handlową innych klientów Przetwarzającego.

5.12. **Profilowanie [art. 13 i 14 RODO**]. Jeżeli Przetwarzający wykorzystuje w celu realizacji Umowy zautomatyzowane przetwarzanie, w tym profilowanie, o którym mowa w art. 22 ust. 1 i 4 RODO. Przetwarzający informuje o tym Administratora w celu i w zakresie niezbędnym do wykonania przez Administratora obowiązku informacyjnego.

5.13. **Szkolenie personelu.** Przetwarzający ma obowiązek zapewnić osobom upoważnionym do przetwarzania danych odpowiednie szkolenie z zakresu ochrony danych osobowych.

6. **Obowiązki Administratora.** Administrator zobowiązany jest współdziałać z Przetwarzającym w wykonaniu Umowy, udzielać Przetwarzającemu wyjaśnień w razie wątpliwości co do legalności poleceń Administratora, jak też wywiązywać się terminowo ze swoich szczegółowych obowiązków.

7. **Bezpieczeństwo danych**

7.1. **Bezpieczeństwo danych osobowych [art. 32 RODO**]. Przetwarzający przeprowadził analizę ryzyka przetwarzania powierzonych Danych i stosuje się do jej wyników co do organizacyjnych i technicznych środków ochrony danych.

7.2. **Środki bezpieczeństwa.** Strony uzgodniły poziom zabezpieczeń Danych wymagany po stronie Przetwarzającego.

7.3. Przetwarzający zapewnia i zobowiązuje się, że:

7.3.1. dokonał oceny przydatności pseudominizacji i szyfrowania i stosuje te techniki w takim zakresie, w jakim są potrzebne do zapewnienia poziomu bezpieczeństwa danych odpowiedniego do ustalonego ryzyka naruszenia praw lub wolności osób, przy ich przetwarzaniu **(o ile dotyczy)**

7.3.2. posiada zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności swoich systemów i usług przetwarzania;

7.3.3. posiada zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;

7.3.4. regularnie testuje, mierzy i ocenia skuteczność stosowanych środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

8. **Gwarancje bezpieczeństwa.** Przetwarzający przedstawił Administratorowi informacje i dokumenty potwierdzające, że Przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych.

9. **Powiadomienie o Naruszeniach Danych Osobowych**

9.1. **Powiadomienie o naruszeniu.** Przetwarzający powiadamia Administratora o każdym podejrzeniu naruszenia ochrony danych nie później niż w 24 godziny od pierwszego zgłoszenia, umożliwia Administratorowi uczestnictwo w czynnościach wyjaśniających i informuje Administratora o ustaleniach z chwilą ich dokonania, w szczególności o stwierdzeniu naruszenia lub jego braku.

9.2. **Rozwinięcie.** Przetwarzający przesyła powiadomienie o stwierdzeniu naruszenia wraz z wszelką niezbędną dokumentacją dotyczącą naruszenia, aby umożliwić Administratorowi spełnienie obowiązku powiadomienia organu nadzoru.

10. **Sprawowanie kontroli [art. 28 ust. 3 lit. h RODO**].
    10.1. **Prawo do kontroli**. Administrator zastrzega sobie prawo do przeprowadzania kontroli, czy przetwarzanie przez Podmiot Przetwarzający powierzonych danych osobowych jest zgodne z postanowieniami Umowy i przepisami obowiązującego prawa.
    10.2. **Dostęp do pomieszczeń**. W trakcie kontroli przedstawiciele Administratora będą mieli prawo do wstępu do pomieszczeń Podmiotu Przetwarzającego, w których są przetwarzane powierzone dane osobowe, po uprzednim uzgodnieniu, z Podmiotem Przetwarzającym stosownie do okoliczności terminu kontroli.
    10.3. **Termin kontroli.** Podmiot Przetwarzający będzie informowany o terminie kontroli z wyprzedzeniem minimum 7 dni (słownie siedmiu dni). Powiadomienie o kontroli będzie określało przedmiot kontroli oraz wskazanie osób upoważnionych do prowadzenia kontroli w imieniu Administratora.
    10.4. **Zakres kontroli.** Kontrola przedstawicieli Administratora określona w ust. 5.1 może dotyczyć wyłącznie sposobu przetwarzania powierzonych danych osobowych, wglądu do dokumentacji wymaganej przez przepisy RODO, przeprowadzania oględzin nośników i systemów teleinformatycznych służących do przetwarzania powierzonych danych osobowych oraz ingerencji w system teleinformatyczny przetwarzający dane w celu weryfikacji zabezpieczeń stosowanych przy przetwarzaniu powierzonych danych osobowych. Kontrola może także dotyczyć jakichkolwiek innych okoliczności faktycznych wzbudzających uzasadnione wątpliwości Administratora.
    10.5. **Protokół z kontroli.** Z kontroli zostanie sporządzony protokół podpisany przez obie Strony, którego jeden egzemplarz zatrzyma Podmiot Przetwarzający.
    10.6. **Zastrzeżenia do protokołu**. Podmiot Przetwarzający może wnieść zastrzeżenia do protokołu z kontroli w ciągu 7 dni roboczych od daty jego podpisania, przez Strony.
    10.7. **Współpraca przy kontroli [art. 28 ust. 3 lit. h RODO**]. Przetwarzający współpracuje z urzędem ochrony danych osobowych w zakresie wykonywanych przez niego zadań.

11. **Oświadczenia Stron**
    11.1. **Oświadczenie Administratora**. Administrator oświadcza, że jest Administratorem danych oraz że jest uprawniony do ich przetwarzania w zakresie, w jakim powierzył je Przetwarzającemu.
    11.2. **Oświadczenie Przetwarzającego [art. 28 ust. 1 RODO].** Przetwarzający oświadcza, że w ramach prowadzonej działalności gospodarczej profesjonalnie zajmuje się przetwarzaniem danych osobowych objętym Umową i Umową Podstawową, posiada w tym zakresie niezbędną wiedzę, odpowiednie środki techniczne i organizacyjne oraz daje rękojmię należytego wykonania niniejszej Umowy.

12. **Odpowiedzialność**
    12.1. **Odpowiedzialność Przetwarzającego [art. 82 ust. 3 RODO]**.Przetwarzający odpowiada za szkody spowodowane swoim działaniem w związku z niedopełnieniem obowiązków, które RODO nakłada bezpośrednio na Przetwarzającego, lub gdy działał poza zgodnymi z prawem instrukcjami Administratora lub wbrew tym instrukcjom. Przetwarzający odpowiada za szkody spowodowane zastosowaniem lub niezastosowaniem właściwych środków bezpieczeństwa.
    12.2. **Odpowiedzialność za Podprocesora [art. 28 ust. 4 RODO**]. Jeżeli Podprocesor nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Administratora za wypełnienie obowiązków przez Podprocesora spoczywa na Przetwarzającym.

13. **Zawiadomienie.** Podmiot przetwarzający niezwłocznie informuje Administratora o wszystkich postępowaniach, w szczególności administracyjnych i sądowych, dotyczących przetwarzania danych osobowych w zakresie danych powierzonych Podmiotowi przetwarzającemu (lub Podprocesorowi), oraz o wszystkich decyzjach administracyjnych i sądowych dotyczących przetwarzania danych, a także o kontrolach dotyczących przetwarzania danych w zakresie powierzenia

14. **Okres Obowiązywania Umowy Powierzenia [art. 28 ust. 3 RODO**] Umowa została zawarta na czas obowiązywania Umowy Podstawowej z zastrzeżeniem terminu karencji usunięcia danych wskazanego w kolejnym artykule Umowy.
15. **Usunięcie danych**
    15.1. **Usunięcie danych [art. 28 ust. 3 lit g RODO].** Z chwilą rozwiązania Umowy Przetwarzający nie ma prawa do dalszego przetwarzania powierzonych danych i jest zobowiązany do usunięcia danych i poinformowania Administratora na piśmie o dacie i sposobie, w jaki usunięto dane, usunięcia wszelkich istniejących kopii lub zwrotu danych, chyba że Administrator postanowi inaczej lub prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują dalej przechowywanie danych,
    15.2. **Karencja**. Przetwarzający dokona usunięcia Danych po upływie 30 dni od zakończenia Umowy Podstawowej, chyba że Administrator poleci mu to uczynić wcześniej.
16. **Postanowienia końcowe**
    16.1. **Pierwszeństwo.** W razie sprzeczności między postanowieniami niniejszej Umowy Powierzenia a Umowy Podstawowej pierwszeństwo mają postanowienia Umowy Powierzenia. Oznacza to także, że kwestie dotyczące przetwarzania danych osobowych między Administratorem a Przetwarzającym należy regulować przez zmiany niniejszej Umowy lub w wykonaniu jej postanowień.
    16.2. **Forma zmian.** Wszelkie zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.
    16.3. **Właściwość prawa.** Wszelkie spory mogące powstać w związku z realizacją przedmiotowej umowy rozstrzygać będzie sąd właściwy dla siedziby Administratora. W sprawach nieuregulowanych mają zastosowanie przepisy dotyczące ochrony danych osobowych (w szczególności RODO).
    16.4. **Adresy Stron do powiadomień i kontakt**. Wszelkie oświadczenia woli, zawiadomienia i inne informacje przekazywane przez jedną Stronę drugiej, będą miały formę pisemną i będą przesyłane za pośrednictwem listu poleconego lub doręczone za pośrednictwem kuriera na odpowiedni adres Strony wskazany poniżej, chyba że Umowa stanowi inaczej:

Administrator	…… ul. …….. ..-… ……
Podmiot przetwarzający	…… ul. …….. ..-… ……
Ponadto na potrzeby realizacji Umowy ustanawia się następujące osoby kontaktowe:	
Administrator	Pan/Pani …….. e-mail: …… tel: ……..
Podmiot przetwarzający	Pan/Pani …… e-mail: …….. tel: …….

16.5. **Egzemplarze**. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

16.6. **Obowiązywanie.** Niniejsza umowa wchodzi w życie z dniem podpisania i zastępuje wszelkie wcześniej zawarte umowy dotyczące powierzenia przetwarzania danych osobowych.

_____	_____
Administrator	Podmiot przetwarzający

ZAŁĄCZNIK NR 11 – WZÓR REJESTRU KATEGORII CZYNNOŚCI PRZETWARZANIA

	1	2	3	4	5	6	8	9	10	11
LP.	Kategorie przetwarzań	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (jeżeli jest to możliwe)	Administrator				Nazwy państw trzecich lub organizacji międzynarodowych, do których dane są przekazywane	Dokumentacja odpowiednich zabezpieczeń danych osobowych przekazywanych na podstawie art. 49 ust. 1 akapit drugi	Podprzetwarzający (podwykonawca) - jeśli dotyczy	
			Nazwa i dane kontaktowe administratora	Nazwa i dane kontaktowe współadministratora (jeśli dotyczy)	Nazwa i dane kontaktowe przedstawiciela administratora (jeśli wyznaczono)	Inspektor ochrony danych administratora (jeśli powołano)			Nazwa i dane kontaktowe podprzetwarzającego (podwykonawcy)	Kategorie podpowierzonych przetwarzań
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										

ZAŁĄCZNIK NR 12 – WZÓR REJESTRU CZYNNOŚCI PRZETWARZANIA

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
LP.	**Nazwa czynności przetwarzania**	**Cel przetwarzania**	**Kategorie osób**	**Kategorie danych**	**Podstawa prawna**	**Źródło danych**	**Planowany termin usunięcia kategorii danych** *(jeżeli jest to możliwe)*	**Nazwa podmiotu przetwarzającego i dane kontaktowe** *(jeśli dotyczy)*	**Kategorie odbiorców** *(innych niż podmiot przetwarzajacy)*	**Nazwa systemu lub oprogramowania**	**Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie z art. 32 ust. 1** ***(jeżeli jest to możliwe)***	**DPIA (jeśli tak, lokalizacja raportu)**	Transfer do kraju trzeciego lub org. międzynarodowej	
													Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)	**Jeśli transfer i art. 49 ust. 1 akapit drugi - dokumentacja odpowiednich zabezpieczeń**
		Art.. 30 ust. 1 pkt b	**Art.. 30 ust. 1 pkt c**	**Art.. 30 ust. 1 pkt c**			**Art.. 30 ust. 1 pkt f**	**Art.. 30 ust. 1 pkt d**	**Art.. 30 ust. 1 pkt d**		**Art.. 30 ust. 1 pkt g**		**Art. 30 ust. 1 pkt e**	**Art. 30 ust. 1 pkt e**
1.														
2.														
3.														
4.														
5.														