POLITYKA OCHRONY DANYCH OSOBOWYCH

BIT Nieruchomości Żych Arkadiusz

1. Nazwa: Arkadiusz Żych prowadzący działalność gospodarczą pod firmą Firma BIT Nieruchomości Żych Arkadiusz (Administrator Danych Osobowych)
2. NIP: 7642551917
3. Regon: 360330891
4. Adres: ul. I Dywizji Wojska Polskiego, nr 3/1, 78 – 520 Złocieniec

Wprowadzenie

1. Polityka bezpieczeństwa ochrony danych osobowych została utworzona w związku z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych - dalej RODO), jak również ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych .
2. Niniejszy dokument obejmuje swoim zakresem:
   a) prawa i obowiązki Administratora danych osobowych w zakresie przetwarzania pozyskiwanych bezpośrednio lub pośrednio danych osobowych,
   b) zasady i reguły postępowania, które należy stosować w celu właściwego zabezpieczenia danych osobowych.
3. Zasady określone w Polityce ochrony danych osobowych mają zastosowanie do:
   - danych osobowych przetwarzanych przez Administratora danych osobowych,
   - wszystkich nośników informacji, np. papierowych, magnetycznych, optycznych itp., na których są lub będą znajdować się dane osobowe podlegające ochronie;
   - wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane dane osobowe podlegające ochronie,
   - wszystkich pracowników tj. osoby zatrudnione na podstawie stosunku pracy, umów cywilnoprawnych (umowa o dzieło, umowa zlecenia), przedsiębiorcy wykonujący działalność osobiście i jednoosobowo, osoby odbywające praktyki, stażyści, osoby skierowane do pracy w ramach umów z agencjami pracy tymczasowej mających dostęp do danych osobowych podlegających ochronie.
4. Dokument Polityki ochrony danych osobowych dotyczy zadań związanych z zabezpieczeniem danych osobowych zarówno przetwarzanych w sposób tradycyjny (papierowy) jak i w systemach informatycznych. Osoby będące pracownikami Administratora Danych Osobowych, zobowiązani są do przestrzegania postanowień w/w dokumentu.
5. Przetwarzanie danych osobowych przez Administratora danych osobowych jest możliwe pod warunkiem, że odbywa się ono zgodnie z wymogami obowiązujących przepisów

z zakresu ochrony danych osobowych oraz niniejszej Polityki ochrony danych osobowych.

6. Przetwarzanie danych osobowych przez Administratora danych osobowych odbywa się z zastosowaniem środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.
7. Każdy Pracownik oraz Współpracownik Administratora danych osobowych ma obowiązek chronić dane osobowych przed dostępem do nich osób nieupoważnionych, nieuzasadnionym modyfikowaniem lub zniszczeniem, ujawnieniem lub pozyskaniem przez podmioty nieupoważnione.
8. Naruszanie RODO zagrożone jest administracyjną karą pieniężną w wysokości do 20 mln euro a w przypadku przedsiębiorstwa do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego.

I. Informacje ogólne z zakresu ochrony danych osobowych

1. Osoby zaangażowane w proces przetwarzania danych osobowych:

   a) Administrator Danych Osobowych (ADO) - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.
   b) Osoby upoważnione do przetwarzania danych osobowych - osoba zatrudniona przez ADO na podstawie umowy o pracę oraz świadcząca usługi na rzecz ADO na podstawie umów cywilnoprawnych, osoba odbywająca praktyki, osoba skierowana do pracy w ramach umów z agencjami pracy tymczasowej wykonująca pracę związaną z przetwarzaniem danych osobowych u ADO na podstawie wydanego dokumentu upoważnienia do przetwarzania danych osobowych.
   c) Podmiot przetwarzający dane – podmiot, który w imieniu ADO przetwarza powierzone na podstawie umowy dane osobowe w celu wskazanym przez ADO, zapewniając wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniło wymogi RODO i chroniło prawa osób, których dane dotyczą.
   d) PUODO – Prezes Urzędu Ochrony Danych Osobowych.

2. Rodzaje przetwarzanych danych osobowych, tj. informacji 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 :
   a) zwykłe - np. imię i nazwisko, imiona rodziców, data i miejsce urodzenia, adres zamieszkania lub pobytu, PESEL, NIP, seria i nr dowodu osobistego, nr telefonu, nr IP komputera, adres poczty elektronicznej, numer rachunku bankowego
   b) szczególnej kategorii - np. nałogi, życie seksualne, stan zdrowia, przekonania religijne,
3. Zbiór danych osobowych - uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest

scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie,

U ADO występują następujące zbiory danych osobowych:

- zbiór pracowników,
- zbiór kandydatów do pracy,
- zbiór kandydatów do współpracy,
- zbiór klientów,
- zbiór dostawców,
- zbiór marketingowy,

4. Nośniki danych osobowych i systemy informatyczne, w tym programy komputerowe – Załącznik do dokumentu
5. Rodzaje czynności podejmowanych w ramach przetwarzania danych osobowych, które rozumiemy jako 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.
6. Profilowanie - dowolna formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

   ADO nie prowadzi profilowania.
7. Formy elektroniczne przetwarzania danych osobowych:
   a) przechowywanie danych na nośnikach elektronicznych (komputery, spartphony, pendrive, dyski zewnętrzne)
   b) hosting poczty elektronicznej i strony www
   c) usługi chmurowe
   d) poczta e – mail
   e) Google
   f) Cookies
8. Cele i podstawy przetwarzania danych osobowych:
   a. osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
   b. przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
   c. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
   d. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
   e. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.
9. Okres przetwarzania danych osobowych – w zależności od podstawy przetwarzania (do czasu odwołania zgody, ustawowy termin, realizacja celu, w jakim pozyskane zostały dane osobowe)
10. Obszar przetwarzania danych osobowych

    Obszarem przetwarzania danych osobowych stanowią pomieszczenia biura ADO zlokalizowane w lokalu nr 1 w budynku przy ul. I Dywizji Wojska Polskiego w Złocieńcu oraz w lokalu nr ..... przy ul. Generała Andersa 9 w Wałczu. Wszystkie pomieszczenia i budynki stanowiące obszar przetwarzania danych osobowych,

w których przetwarzane są dane osobowe zabezpieczone są drzwiami głównymi do biura oraz drzwiami do poszczególnych pomieszczeń, zamykanych na klucz. Wykaz pomieszczeń, w których przetwarzane są dane osobowe stanowi załącznik do niniejszej Polityki ochrony danych.

11. Zlecenie przetwarzania danych osobowych:

    a. Administrator danych osobowych może powierzać przetwarzanie danych osobowych innemu podmiotowi w drodze umowy zawartej w formie pisemnej.
    b. Podmiot, z którym zawarta jest umowa powierzenia przetwarzania danych, jest zobowiązany do spełnienia warunków wskazanych w RODO, celem prawidłowego zabezpieczenia powierzonych danych osobowych przez ADO.
    c. Podmioty, z którymi zostały zawarte umowy powierzenia danych osobowych (zgodnie z załącznikiem).
12. Przetwarzanie danych osobowych poza obszarem Unii Europejskiej – nie dotyczy ADO

II. Obowiązki Administratora Danych Osobowych

1. Sposób realizacji obowiązków informacyjnych wobec osoby, której dane osobowe dotyczą
    a. ADO podejmuje odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem – w szczególności gdy informacje są kierowane do dziecka – udzielić osobie, której dane dotyczą, wszelkich informacji, wskazanych w art. 13 i 14 RODO. Informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą.
    b. Elementy składowe obowiązku informacyjnego: tożsamość i dane kontaktowe ADO, tożsamość i dane kontaktowe swojego przedstawiciela lub inspektora ochrony danych, cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania, wskazanie, jeżeli dotyczy, prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu, informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych, informacje o prawie do cofnięcia zgody, jeżeli dotyczy, w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem, informacje o prawie wniesienia skargi do organu nadzorczego, informację, 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.
    c. ADO bez zbędnej zwłoki – a w każdym razie w terminie miesiąca od otrzymania żądania – udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku ze złożonym żądaniem. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od

otrzymania żądania administrator informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.

d. Informacje zgodnie z RODO oraz komunikacja i działania ADO na rzecz osoby, której dane dotyczą, są wolne od opłat, chyba, że są ewidentnie nieuzasadnione lub nadmierne. W zaistniałej sytuacji ADO może pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań lub odmówić podjęcia działań w związku z żądaniem.

2. Sposób realizacji obowiązków informacyjnych w przypadku, gdy dane osobowe nie są pozyskiwane od osoby, której dane dotyczą
   a. ADO realizuje wtórny obowiązek informacyjny w postaci podania osobie, której dane dotyczą, informacje takie jak: tożsamość i dane kontaktowe ADO, dane kontaktowe swojego przedstawiciela lub inspektora ochrony danych, cele przetwarzania, do których mają posłużyć dane osobowe, oraz podstawę prawną przetwarzania, kategorie odnośnych danych osobowych, informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją, gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony, okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu, prawnie uzasadnione interesy (jeżeli dotyczy) realizowane przez administratora lub przez stronę trzecią, informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych, informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem (jeżeli dotyczy), informacje o prawie wniesienia skargi do organu nadzorczego, źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych, informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu.
   b. Informacje wskazane powyżej ADO podaje w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca – mając na uwadze konkretne okoliczności przetwarzania danych osobowych lub jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą lub jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.
3. Sposoby uzyskiwania zgody na przetwarzanie danych osobowych- drogą mailową, pisemnie, telefonicznie.
4. Procedura wycofania zgody na przetwarzanie danych osobowych:
   a. Drogą mailową na adres: **biuro@bit-nieruchomosci.pl**
   b. Pocztą tradycyjną na adres: **ul.I Dywizji Wojska Pol. 3/1, 78-520 Złocieniec**
   c. Telefonicznie pod nr tel.: **691191005**
5. Prawa związane z danymi osobowymi:
   a. procedura weryfikacji tożsamości zgłaszającego
   b. samodzielna zmiana danych w systemie informatycznym
   c. prawo dostępu do danych osobowych
   d. prawo do sprostowania danych osobowych
   e. prawdo do usunięcia danych osobowych (prawo do bycia zapomnianym)
   f. prawdo do ograniczenia przetwarzania danych
   g. prawo do uzyskiwania pliku danych i przenoszenia danych osobowych
   h. prawo do sprzeciwu wobec przetwarzania danych osobowych

i. procedura przyjmowania i rozpatrywania żądań oraz udzielania odpowiedzi

III. Ochrona danych osobowych pracowników

1. Dane osobowe potencjalnych pracowników są przetwarzane przez ADO. Po przeprowadzeniu procesu rekrutacyjnego dane osób w postaci CV oraz listu motywacyjnego, które nie przeszły pozytywnie naboru zostają usunięte (forma papierowa i elektroniczna – zgodnie z procedurą). Dane osób, które przeszły pozytywnie proces rekrutacyjny pozostają w biurze ADO. Dane pozostałych osób biorących udział w procesie rekrutacyjnym są niezwłocznie niszczone. W przypadku wyrażenie zgody na przetwarzanie danych osobowych dla celów przyszłych rekrutacji, złożone przez zainteresowaną osobę dokumenty zawierające dane osobowe przechowywane są w formie papierowej.
2. Dane osobowe pracowników przetwarzane są zgodnie z art. 6 ust.1 lit b), c), d), f) RODO:
   a. przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
   b. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
   c. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
   d. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

      Dane osobowe pracowników oraz współpracowników ADO przetwarzane są na podstawie umowy powierzenia przetwarzania danych osobowych przez podmiot zewnętrzny.

IV. Procedury wewnętrzne Administratora Danych Osobowych

Procedura procesu rekrutacyjnego

1. Ogłoszenie o prowadzonym postępowaniu rekrutacyjnym zamieszczone jest w wybranych serwisach i portalach z ogłoszeniami o pracę.
2. Aplikacje osób na określone stanowisko wpływają bezpośrednio na adres mailowy wskazany w ogłoszeniu, dostarczane są osobiście do siedziby pracodawcy, gdzie są gromadzone i przechowywane do czasu zakończenia postępowania rekrutacyjnego.
3. Dostarczane dokumenty przez kandydatów muszą być zaopatrzone w *klauzulę wyrażenia zgody na przetwarzanie danych osobowych do celów rekrutacyjnych na stanowisko*
4. Po zakończonym procesie rekrutacyjnym:
   a) osoby z którymi został podjęty kontakt, informowane są telefonicznie o wynikach naboru;
   b) CV osób, które nie przeszły pomyślnie etapu rekrutacji są niszczone w niszczarkach - w przypadku wersji papierowej; w przypadku przesłania dokumentów drogą mailową - korespondencja ulega usunięciu zarówno ze skrzynki odbiorczej jak i z kosza poczty elektronicznej.
5. W przypadku wyrażenia zgody przez kandydata na przetwarzanie danych osobowych dla celów przyszłych rekrutacji, jego dane osobowe nie podlegają zniszczeniu (pkt. 7 lit b); mogą być dalej przetwarzane przez okres 3 miesięcy od dnia ogłoszenia o procesie rekrutacyjnym na konkretne stanowisko.

Procedura zakończenia stosunku pracy

1. Rozwiązanie stosunków pracy z pracownikami następuje z przyczyn i zgodnie z procedurami przewidzianymi w stosownych przepisach prawa, w tym Kodeksie pracy.
2. Oświadczenie o rozwiązaniu stosunku pracy sporządza się na piśmie.
3. Bezpośrednio przed wręczeniem oświadczenia przeprowadza się z pracownikiem rozmowę, wyjaśniając mu motywy i przyczyny podjęcia decyzji o rozwiązaniu umowy o pracę.
4. Rozmowę przeprowadza się w warunkach zapewniających zachowanie poufności danych.
5. Podczas rozmowy z pracownikiem, obecne mogą być jedynie osoby upoważnione do przetwarzania danych osobowych w zakresie stosunku pracy.
6. W przypadku odmowy przyjęcia przez pracownika pisemnego oświadczenia o rozwiązaniu stosunku pracy, sporządza się pisemny protokół, z podaniem daty i miejsca rozmowy oraz danych osób w nich uczestniczących.
7. Po zakończeniu biegu okresu wypowiedzenia lub zakończeniu stosunku pracy na skutek rozwiązania umowy o pracę bez wypowiedzenia, pracownikowi doręcza się świadectwo pracy, w terminie przewidzianym przepisami prawa pracy.
8. Świadectwo pracy doręcza się pracownikowi za pośrednictwem poczty (wyłącznie na jego prośbę), przesyłką poleconą za zwrotnym potwierdzeniem odbioru, w zamkniętej, nieprzeźroczystej kopercie lub umożliwia osobisty odbiór w sekretariacie.
9. Na kopercie poza danymi adresowymi pracownika nie umieszcza się żadnych informacji mogących ujawnić charakter i treść korespondencji.
10. W dniu zakończenia stosunku pracy, deaktywuje się dostęp pracownika do przydzielonej mu skrzynki poczty elektronicznej, wszelkie karty i urządzenia pozwalające na dostęp do danych pracodawcy oraz wstęp na teren przedsiębiorstwa.
11. W dniu zakończenia stosunku pracy usuwa się uprawnienia pracownika, z którym rozwiązano stosunek pracy, z ewidencji osób uprawnionych do przetwarzania danych osobowych.

Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności.

1. Każdy pracownik/współpracownik obsługujący system informatyczny musi posiadać pisemne upoważnienie Administratora danych do Przetwarzania danych osobowych, jeśli w ramach podejmowanych działań, przetwarzanie danych będzie konieczne.
2. Przed przystąpieniem do Przetwarzania danych albo wykonywania innych czynności związanych z obsługą systemu informatycznego, pracownik/współpracownik obowiązany jest zgłosić się do Administratora danych i okazać upoważnienie, o którym mowa w pkt 1 powyżej.
3. Administrator danych podejmuje decyzję o dopuszczeniu pracownika/współpracownika do obsługi systemu informatycznego oraz ustala dla pracownika/współpracownika odrębny, niepowtarzalny Identyfikator. Administrator danych niezwłocznie po przydzieleniu Identyfikatora pracownikowi/współpracownikowi, dokonuje rejestracji tego Identyfikatora w systemie informatycznym. Identyfikator nie powinien być zmieniany. Po wyrejestrowaniu pracownika/współpracownika z systemu informatycznego, przydzielony temu Identyfikator nie może być przydzielony innej osobie.
4. Pracownik/współpracownik zobowiązany jest do zachowania szczególnej ostrożności w zakresie posługiwania się Identyfikatorem, w tym w szczególności do przechowywania Identyfikatora w sposób uniemożliwiający jego utratę.
5. Administrator danych wpisuje do ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych następujące dane: imię i nazwisko

pracownika/współpracownika, datę przyznania upoważnienia do przetwarzania danych osobowych oraz zakres tego upoważnienia, a także przydzielony Identyfikator.

6. W sytuacji utraty przez pracownika/współpracownika uprawnień do przetwarzania danych osobowych, w szczególności w razie zmiany stanowiska pracy, zakresu obowiązków, rozwiązania umowy o pracę, Administrator danych dokonuje niezwłocznego wyrejestrowania z systemu informatycznego Identyfikatora pracownika/współpracownika, unieważnia Hasło oraz dokonuje stosownego wpisu w ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych, wskazując między innymi datę ustania upoważnienia pracownika/współpracownika do przetwarzania danych.
7. W przypadkach awaryjnych, rozumianych jako nagłe i nieprzewidziane zagrożenia systemu informatycznego, Administrator danych zobowiązany jest, w zależności od okoliczności awarii, niezwłocznie zabezpieczyć Obszar przetwarzania danych przed dostępem osób nieuprawnionych i/lub zastosować dostępne środki fizyczne lub informatyczne celem usunięcia awarii.
8. Za przebieg procedury nadawania i odbierania pracownikowi/współpracownikowi uprawnienia do przetwarzania danych osobowych odpowiedzialny jest Administrator danych.
9. Za proces rejestrowania i wyrejestrowywania uprawnienia pracownika / współpracownika do przetwarzania danych, dokonywania wpisów w ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych, odpowiedzialny jest Administrator danych.

Procedura kontroli podmiotów przetwarzających – w załączeniu

1. Administratora Danych Osobowych jest uprawniony do kontrolowania sposobu wykonywania przez Procesora umowy przetwarzania danych osobowych.
2. Administratora Danych Osobowych ma prawo kontrolowania, czy Procesor przetwarzając Dane osobowe przestrzega regulacji wskazanych 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 (ogólne rozporządzenie o ochronie danych)- dalej jako RODO, w szczególności w zakresie, w jakim naruszenie tych przepisów mogłoby prowadzić do ponoszenia przez Administratora Danych Osobowych odpowiedzialności, w tym w szczególności naruszałoby prawa osób trzecich lub zagrażałoby bezpieczeństwu Danych osobowych.
3. Administrator Danych Osobowych poinformuje Procesora o planowanej kontroli na 7 dni przed podjęciem czynności w siedzibie Procesora.
4. W celu wykonywania Kontroli osoby pisemnie upoważnione przez Administratora Danych Osobowych mają prawo:
    a. wstępu do obszarów przetwarzania Danych osobowych w godzinach pracy Procesora, tj. 9 -16, w których przetwarzane są Dane osobowe oraz przeprowadzania niezbędnych czynności kontrolnych;
    b. żądania złożenia przez Procesora pisemnych i ustnych wyjaśnień w celu ustalenia stanu faktycznego;
    c. przeprowadzenia oględzin urządzeń, nośników i systemów informatycznych służących do przetwarzania Danych osobowych.
5. Z przeprowadzonej Kontroli sporządzony zostanie protokół w dwóch egzemplarzach, po jednym dla każdej ze Stron.
6. Procesor zapewni niezwłoczną możliwość przeprowadzenia przez Administratora Danych Osobowych kontroli w każdym z obszarów przetwarzania Danych osobowych.
7. W przypadku ujawnienia okoliczności uznanych przez Administratora Danych Osobowych za uchybienia / naruszenia w zakresie przetwarzania Danych osobowych, Procesor zobowiązuje się do ich niezwłocznego usunięcia w terminie wskazanym przez Administratora Danych Osobowych. W przypadku

nieusunięcia przez Procesora uchybień / naruszeń w wyznaczonym przez Administratora Danych Osobowych terminie, może on wypowiedzieć bez zachowania okresu wypowiedzenia zawartą Umowę handlową. Nie zwalnia to Procesora z odpowiedzialności, wskazanej w umowie o powierzeniu danych osobowych.

Procedura weryfikacji zbierania danych osobowych i odrzucania niepotrzebnych danych (adekwatność)

ADO zapewnia, aby przetwarzane dane osobowe były adekwatne w stosunku do celów, w jakich są przetwarzane, czyli niezbędne i wystarczające. W związku z powyższym zapewnienia ograniczenie okresu przechowywania danych do ścisłego i niezbędnego minimum. Aby zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne, ADO ustala termin usuwania danych osobowych pozyskanych w określonym celu, jak również dokonuje ich okresowego przeglądu.

Procedura niszczenia danych na nośnikach elektronicznych

1. Za kasowanie informacji z pamięci masowych serwerów oraz nośników kopii archiwalnych i zapasowych odpowiada wyznaczona przez Administratora Ochrony Danych osoba.
2. Zniszczenie nośnika zostaje odnotowane w protokole zniszczenia, podpisanym przez ADO.
3. W odniesieniu do nośników przenośnych (pen-drive) oraz nośników danych zainstalowanych w komponentach informatycznych, stosowane są następujące mechanizmy bezpiecznego kasowania informacji:
   - za pomocą specjalistycznego oprogramowania
   - przy użyciu demagnetyzacji
   - poprzez fizyczne niszczenie (pocięcie, spalenie) nośników.

Procedura niszczenia danych na nośnikach papierowych

1. Dokumentacja papierowa niszczona jest:
   - na bieżąco w niszczarkach paskowych oraz w niszczarkach o podwyższonym standardzie,
   - za pośrednictwem firmy niszczącej dokumenty.
2. Firma niszcząca dokumenty zobowiązana jest do wykazania się bezpieczną procedurą utylizacji (np. 27001, nagrania z procedur transportu i utylizacji).
3. Każdorazowy proces masowego niszczenia danych przez firmę niszcząca dokumenty musi zostać potwierdzony stosownymi zaświadczeniami.

Procedura przekazywania nośników do serwisu

1. Komputery przeznaczone do naprawy należy wysyłać bez dysków, a urządzenia mobilne bez kart pamięci.
2. W przypadku naprawy sprzętu z danymi osobowymi na nośniku należy je trwale usunąć
   z użyciem specjalistycznego oprogramowania, dokonując przy tym kopi danych w celu późniejszego odtworzenia.
3. W przypadku naprawy sprzętu z danymi osobowymi na nośniku - rekomendowane jest przekazywanie do naprawy uszkodzonego sprzętu z danymi zaszyfrowanymi na dysku / karcie pamięci. Sprzęt przekazywany jest do serwisu bez podania hasła.
4. Rekomendowane jest korzystanie z serwisu, który dokonuje napraw w siedzibie przedsiębiorstwa (umowy gwarancyjne on-site)

5. W przypadku dokonywania napraw w siedzibie przedsiębiorstwa, komputery i urządzenia mobilne naprawiane są w obecności osoby upoważnionej do przetwarzania danych.

Procedura korzystanie z komputerów i innych elektronicznych urządzeń przenośnych

1. W przypadku przechowywania na urządzeniu przenośnym danych osobowych lub stanowiących tajemnicę Administratora Danych Osobowych, Użytkownik zobowiązany jest do ich przechowywania na dysku szyfrowanym, zabezpieczonym co najmniej 8 znakowym hasłem (duże, małe litery, znaki specjalne lub cyfry).
2. Na urządzeniach przenośnych przeznaczonych do zewnętrznych prezentacji multimedialnych nie powinny, o ile jest to możliwe, znajdować się dane osobowe lub stanowiące tajemnicę Administratora Danych Osobowych.
3. W przypadku kradzieży lub zgubienia urządzenia przenośnego, Użytkownik powinien natychmiast (nie później, niż w ciągu 2 godzin) powiadomić o tym Administratora Danych Osobowych, zaznaczając jednocześnie, jakiego rodzaju dane były na tym urządzeniu przechowywane.
4. Użytkownik zobowiązany jest do zabezpieczenia urządzenia przenośnego w czasie transportu, a w szczególności:
   a. zaleca się przenoszenie komputera / tabletu w specjalnym futerale (torbie, pokrowcu)
   b. zabrania się pozostawiania urządzenia przenośnego w samochodzie podczas postoju w miejscu publicznym bez nadzoru.
   c. podczas jazdy samochodem zaleca się przechowywanie komputera przenośnego w bagażniku.
5. W przypadku, gdy komputer przenośny pozostawiony jest w miejscu dostępnym dla osób nieupoważnionych, Użytkownik jest zobowiązany do stosowania kabla zabezpieczającego.
   W szczególności dotyczy to zabezpieczenia komputera na stanowisku pracy, podczas konferencji, prezentacji, szkoleń, targów itp.
6. W przypadku pozostawiania urządzeń przenośnych w biurze zaleca się umieszczanie ich po zakończeniu pracy w zamykanych szafkach.
7. Użytkownik komputera przenośnego jest zobowiązany do regularnego tworzenia kopii bezpieczeństwa danych na serwerze lub na określonych nośnikach (pendrive, CD, DVD). Nośniki z takimi kopiami powinny być przechowywane w bezpiecznym miejscu, z uwzględnieniem ochrony przed dostępem osób niepowołanych.
8. Pracując na urządzeniu przenośnym w miejscach publicznych i środkach transportu, użytkownik zobowiązany jest chronić wyświetlane na monitorze informacje przed wglądem osób nieupoważnionych.
9. Pracując na urządzeniu przenośnym w miejscach publicznych i środkach transportu należy unikać korzystania z publicznie dostępnych, otwartych sieci WIFI.
10. Należy ograniczyć korzystanie z przenośnych nośników informacji typu pendrive do niezbędnego minimum, w szczególności podczas wynoszenia ich poza biuro. W takiej sytuacji, dane osobowe (o ile znajdują się na nośniku) winny zostać zaszyfrowane.
11. Nośniki danych typu pendrive oraz inne nośniki danych pochodzenia obcego, które mają zostać podłączone do komputerów winny być w pierwszej kolejności sprawdzone za pomocą programu antywirusowego.

Procedura szacowania ryzyka

1. W związku z wejściem w życie w dniu 25 maja 2018 r. *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 swobodnym przepływem takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)* obligatoryjnym jest przeprowadzanie okresowych czynności z zakresu szacowania ryzyka.
2. Przy założeniu przestrzegania procedur, prowadzeniem wskazanych przez ustawodawcę rejestrów oraz zastosowaniu właściwych zabezpieczeń technicznych i organizacyjnych, wyniki analizy ryzyka przetwarzania danych osobowych przeprowadzonej w oparciu o dokument „Analiza ryzyka RODO", wskazują, iż ryzyko kształtuje się na poziomie akceptowalnym o niskim indeksie istotności.
3. Szacowanie ryzyka, celem aktualizacji w/w dokumentu odbywa się nie rzadziej niż raz na trzy lata oraz każdorazowo po wystąpieniu istotnego uchybienia lub zagrożenia.
4. Szacowanie ryzyka przeprowadzane jest przez Administratora Danych Osobowych przy współudziale pracowników i współpracowników.

Procedura ciągłości działania systemu informatycznego

1. W przypadku stwierdzenia krytycznej awarii serwera podstawowego w centrali, osoba upoważniona podpina serwer zapasowy, konfiguruje serwer, zgrywa dane z kopii dziennej.
2. Po uruchomieniu serwera podłącza go do sieci.
3. Przewidywany czas operacji uruchomienia serwera zapasowego – 3 godziny
4. W przypadku nieobecności wyznaczonej do w/w czynności osoby, procedurę odtworzenia należy wykonać z pomocą firmy ……, z którą obowiązuje umowa ……..
5. W przypadku zniszczenia miejsca serwerowni wraz z serwerem, należy zaplanowaną uprzednio lokalizację przeznaczyć na alternatywną serwerownię.
6. Przygotowanie serwerowni wymaga: zapewnienia energii elektrycznej, UPS, łącz telekomunikacyjnych.
7. …… jest odpowiedzialny za dostawę serwera zapasowego, jego konfigurację, wgranie danych z kopii zapasowych (zgodnie z wewnętrzną procedurą IT).
8. Po uruchomieniu serwera …… podłącza go do sieci.
9. Przewidywany czas operacji uruchomienia serwera zapasowego – 2 dni
10. W przypadku nieobecności ……..., procedurę odtworzenia należy wykonać z pomocą firmy ……., z którą obowiązuje umowa …….
11. W przypadku niedostępności internetu awarię zgłaszać do …… pod numerem …….
12. W przypadku dłuższej niedostępności internetu, uruchomić router sieci komórkowej ……., tel. Kontaktowy ……..., opiekun ……..

Procedura wykrywania incydentów naruszeń ochrony danych osobowych oraz ich zgłaszania wyznaczonej osobie

Okresowo przeprowadzane są kontrole naruszenia ochrony danych osobowych wynikające z niestosowania obowiązujących przepisów i przekazanej z zakresu ochrony danych osobowych wiedzy. Wykrywanie naruszeń następuje podczas doraźnych kontroli przeprowadzanych w miejscu wykonywania pracy lub realizacji zlecenia. Na bieżąco udzielane są upomnienia oraz weryfikowana wiedza z zakresu ochrony danych osobowych pracowników i współpracowników.

Procedura zgłaszania naruszeń danych osobowych Prezesowi UODO

1. W przypadku naruszenia ochrony danych osobowych, ADO bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, zgłasza je organowi nadzorczemu – Prezesowi Urzędu Ochrony Danych Osobowych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin należy dołączyć wyjaśnienie przyczyn opóźnienia. Zgłoszenie musi zawierać, co najmniej:
   a. opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
   b. imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
   c. możliwe konsekwencje naruszenia ochrony danych osobowych;
   d. 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.
2. Administrator Danych Osobowych jest zobowiązany do dokumentowania wszelkich naruszeń ochrony danych osobowych, w tym okoliczności ich naruszenia, skutki oraz podjęte działania zaradcze.

Procedura powiadamiania o naruszeniu danych osobowych zainteresowanego

1. W sytuacji, gdy naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, ADO bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu. Przedmiotowe zawiadomienie musi być napisane językiem jasnym, prostym i zrozumiałym dla ogółu. Należy wskazać charakter naruszenia ochrony danych osobowych oraz informacje dotyczące punktu (osoby) kontaktowego, możliwe konsekwencje naruszenie danych osobowych oraz zastosowane środki zaradcze.
2. Zawiadomienie nie jest wymagane, gdy Administrator Danych Osobowych:
   a. 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,
   b. zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
   c. poniósł by niewspółmiernie duży wysiłek.
3. W przypadku zaistnienia powyższej sytuacji należy wydać publiczny komunikat lub zastosować podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w skuteczny sposób.

Procedura dostępu do pomieszczeń biura – polityka kluczy

1. Każdy pracownik/ współpracownik, w dniu podjęcia pracy / współpracy z Administratorem Danych Osobowych otrzymuje klucze umożliwiające dostęp do pomieszczeń biurowych.
2. Wydanie kluczy następuje po dokonaniu wpisu do Ewidencji dostępu do pomieszczeń biurowych zawierającej:
   a. imię i nazwisko osoby, której wydane zostają klucze,
   b. datę wydania kluczy,
   c. wykaz udostępnionych pomieszczeń indywidualnej osobie,
   d. podpis osoby otrzymującej klucze
   e. datę zdania kluczy
3. Klucze zapasowe znajdują się w ……..
4. Zdanie kluczy następuje po zakończeniu stosunku pracy lub umowy o współpracę wraz ze wskazaniem daty zdania kluczy.

5. Osoby nie wskazane w Ewidencji dostępu do pomieszczeń biurowych, mogą przebywać w nich wyłącznie w obecności osób uprawnionych.
6. Klucze do pomieszczeń pozostają pod osobistym nadzorem osób upoważnionych.
7. Zabrania się pozostawiania kluczy w biurkach i szafach podczas chwilowej nieobecności osób upoważnionych w pomieszczeniu.
8. Po zakończeniu pracy, klucze służące do zabezpieczenia biurek i szaf muszą być przechowywane w zabezpieczonym miejscu
9. Po zakończeniu pracy pracownicy/współpracownicy są zobowiązani do zabezpieczenia pomieszczeń, w szczególności wyłączenia i zabezpieczenia urządzeń elektronicznych oraz elektrycznych, wyłączenia oświetlenia, zabezpieczenia i zamknięcia okien i drzwi.

Privacy by design i privacy by default

1. Stosowanie zasady „privacy by design" przez ADO polega na obowiązku uwzględniania zagadnień ochrony danych osobowych, prywatności osób, których dane dotyczą, już na etapie projektowania i opracowywania sposobów przetwarzania danych a ponadto na każdym następnym etapie ich przetwarzania. Środkami służącymi do realizacji w/w zasady są : minimalizacja przetwarzanych danych osobowych, jak najszybsza pseudonimizacja, przejrzystość co do funkcji przetwarzania danych osobowych, umożliwienie osobie, której dane dotyczą monitorowania przetwarzania danych, umożliwienie administratorowi tworzenia i doskonalenia zabezpieczeń.
2. Zasada domyślnej ochrony danych „privacy by default" polega na wdrożeniu przez administratora danych odpowiednich środków technicznych i organizacyjnych w celu domyślnego przetwarzania wyłącznie danych, 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 osoby, nieokreślonej liczbie osób fizycznych. Ustawienia prywatności danych mają na celu maksymalną ochronę użytkownika. Generalna zasada dotyczy maksymalnej ochrony prywatności danych, odstępstwem – na wyraźne żądanie użytkownika – będzie umożliwienie dostępu do określonych, wskazanych danych osobowych określonym osobom lub podmiotom.

Procedura monitorowania i uaktualniania dokumentów z zakresu ochrony danych osobowych oraz stosowanych środków ochrony danych osobowych.

Administrator danych osobowych prowadzi ciągły monitoring zmian legislacyjnych w zakresie ochrony danych osobowych, w tym wytycznych Prezesa Urzędu Ochrony Danych Osobowych i w miarę potrzeby aktualizuje dokumentację ochrony danych osobowych.

Procedura wysyłanie korespondencji elektronicznej

1. Redagując wiadomość e-mail, w pierwszej kolejności należy przygotować jej treść. Wpisanie adresu poczty elektronicznej adresata następuje na końcu. Wysłanie wiadomość musi zostać poprzedzone sprawdzeniem, czy na liście adresatów nie ma osób, do których korespondencja nie jest adresowana.
2. Przy wysyłaniu korespondencji zewnętrznej (do adresatów innych, niż pracownicy), do większej liczby adresatów, jako zasadę należy przyjąć używanie funkcji UDW (ukryte do wiadomości).
3. Powyższe nie dotyczy sytuacji, gdy adresatami korespondencji są również wpisywania pracownicy Administratora. W takiej sytuacji, adresy pracowników

Administratora należy wpisać w polu „do” lub „dw (do wiadomości), a pozostałe adresy w polu „UDW”.
4. Powyższe nie dotyczy również sytuacji, w której korespondencja wysyłana jest do większej liczby adresatów, jednakże są to pracownicy jednego podmiotu lub organizacji.
5. Pracownik oświadcza, że będzie wykorzystywał swój służbowy adres poczty wyłącznie w celu prowadzenia korespondencji związanej z działalnością administratora.

Polityka czystego biurka

1. Każdy pracownik/współpracownik zobowiązany jest do przechowywania na biurku tylko tych dokumentów, które są mu niezbędne do pracy w danym momencie.
2. Należy unikać przechowywania dokumentów niepotrzebnych do bieżących zadań.
3. Po zakończeniu pracy z dokumentami zawierającymi dane osobowe należy odłożyć je do szuflady lub szafy zamykanej na klucz.
4. Dokumenty niepotrzebne w dalszej pracy i niepodlegające archiwizacji należy niszczyć zgodnie z zaleceniami „Procedury niszczenia dokumentów”
5. Ekrany monitorów komputerów powinny być ustawione tak by uniemożliwiały widok osobom postronnym.
6. Na biurku nie powinny znajdować się napoje w pojemnikach grożących rozlaniem.
7. Po zakończeniu pracy na biurku nie powinny pozostać dokumenty

Szkolenia

1. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.
2. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami RODO, ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz Polityką bezpieczeństwa i innymi związanymi z nią dokumentami obowiązującymi u administratora danych osobowych,
3. Szkolenie zostaje zakończone podpisaniem przez słuchacza oświadczenia o wzięciu udziału w szkoleniu i jego zrozumieniu oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych.
4. Administrator danych monitoruje zmiany stanu prawnego w zakresie danych osobowych i w miarę potrzeby organizuje szkolenia dla osób przetwarzających dane osobowe.

V. <u>Prowadzone przez ADO rejestry i ewidencje:</u>

1. Rejestr czynności przetwarzania danych osobowych
2. Rejestr naruszeń ochrony danych osobowych oraz incydentów bezpieczeństwa danych
3. Ewidencja osób upoważnionych do przetwarzania danych osobowych i ich uprawnień
4. Ewidencja nośników danych osobowych oraz programów komputerowych
5. Wykaz pomieszczeń, w których przetwarzane są dane osobowe
6. Lista osób uprawnionych do pomieszczeń biurowych
7. Rejestr umów powierzenia danych osobowych (Wykaz podmiotów, którym powierzono przetwarzanie danych osobowych)

8. Środki zabezpieczeń danych osobowych poza systemami informatycznymi
9. Środki zabezpieczeń danych osobowych w systemach informatycznych

VI. Środki bezpieczeństwa przetwarzania danych osobowych

1. Zabezpieczenia organizacyjne
   a. opracowano i wdrożono niniejszą Politykę bezpieczeństwa,
   b. stworzono procedurę postępowania w sytuacji naruszenia ochrony danych osobowych,
   c. opracowano i bieżąco prowadzi się rejestr czynności przetwarzania
   d. do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora danych bądź osobę przez niego upoważnioną,
   e. osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego,
   f. osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy,
   g. przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych,
   h. przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych,
   i. dokumenty i nośniki informacji zawierające dane osobowe, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonuje się takiej ich modyfikacji, która nie pozwoli na odtworzenie ich treści.

2. Zabezpieczenia techniczne

   a. wewnętrzną sieć komputerową zabezpieczono poprzez odseparowanie od sieci publicznej wykaz środków technicznych stanowi załącznik do niniejszej polityki
   b. stanowiska komputerowe wyposażono w indywidualną ochronę antywirusową,
   c. komputery zabezpieczono przed możliwością użytkowania przez osoby nieuprawnione do przetwarzania danych osobowych, za pomocą indywidualnego identyfikatora użytkowania i cykliczne wymuszanie zmiany hasła.

3. Środki ochrony fizycznej:

   a. obszar, na którym przetwarzane są dane osobowe, poza godzinami pracy, chroniony jest przed dostępem osób nieuprawnionych przez zamykane drzwi antywłamaniowe, domofon oraz zamykane na zamek drzwi do poszczególnych pomieszczeń.
   b. urządzenia służące do przetwarzania danych osobowych umieszczone są w zamykanych pomieszczeniach,
   c. dokumenty i nośniki informacji zawierające dane osobowe przechowywane są w zamykanych na klucz szafach.

VII. Wzory dokumentów

1. Wzór protokołu usunięcia danych osobowych ze zbioru danych – w załączeniu

2. Wzór klauzuli obowiązku informacyjnego- w załączeniu
3. Wzór umowy powierzenia przetwarzania danych osobowych- w załączeniu
4. Wzór protokołu zniszczenia uszkodzonych nośników komputerowych – w załączeniu
5. Wzór oświadczenia pracownika/współpracownika w zakresie ochrony danych osobowych- w załączeniu
6. Wzór oświadczenia w sprawie zasad ochrony danych osobowych i odpowiedzialności za prawidłowe przetwarzanie w indywidualnym zakresie czynności – wzór w załączeniu
7. Wzór upoważnienia do przetwarzania danych osobowych – w załączeniu
8. Wzór rejestru pracowników upoważnionych do przetwarzania danych osobowych – w załączeniu
9. Wzór arkuszu szacowania ryzyka – w załączeniu
10. Wzór formularza rejestracji incydentu- w załączeniu
11. Wzór zawiadomienia o naruszeniu ochrony danych osobowych