Polityka ochrony danych osobowych
w IT CONNECT Sp. z o.o.

Wersja 3.0

I. POSTANOWIENIA OGÓLNE

§1.
Przedmiot Polityki

1. IT CONNECT Spółka z ograniczoną odpowiedzialnością jest Administratorem Danych Osobowych w rozumieniu art. 4 pkt 7 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 z dnia 4 maja 2016 r.).
2. W celu zapewnienia przetwarzania danych osobowych przez Administratora Danych Osobowych zgodnie z obowiązującym prawem, a w szczególności zapewnienia najwyższej ochrony przetwarzanych danych osobowych, Administrator Danych Osobowych przyjmuje niniejszą Politykę.
3. Niniejsza Polityka jest zgodna z:
   a) 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) (Dz. U. UE L z dnia 4 maja 2016 r. — dalej: RODO);
   b) ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych— dalej: u.o.d.o.);
   c) ustawą z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t. j. Dz. U. 2017 poz. 1219, z późn. zm. — dalej: u.ś.u.d.e.);
   d) ustawą z dnia 26 czerwca 1974 r. — Kodeks pracy (t. j. Dz. U. 2018 poz. 108, z późn. zm. — dalej: k.p.);
4. Polityka stanowi część składową systemu ochrony danych osobowych obowiązującego u Administratora Danych Osobowych, określając w szczególności:
   a) zasady przetwarzania danych osobowych u Administratora Danych Osobowych;
   b) zasady zapewniania ochrony przetwarzanych danych osobowych;
   c) procedury stosowane u Administratora Danych Osobowych;
   d) wzorce dokumentów i formularzy stosowanych przez Administratora Danych Osobowych;
   e) wzorce klauzul informacyjnych;
   f) wzorce klauzul zgody.
5. Niniejsza Polityka jest środkiem prawnym przewidzianym w art. 24 ust. 2 RODO.

§2.
Słowniczek

Na potrzeby niniejszej Polityki przyjmuje się następujące definicje użytych pojęć:

Pojęcie	Definicja
Administrator Danych Osobowych	IT CONNECT Sp. z o.o., Marszałkowska 80 Warszawa 00-517, Polska. Sąd Rejonowy dla m. st. Warszawy w Warszawie XII Wydział Gospodarczy Krajowego Rejestru Sądowego. NR KRS 0000277350; REGON: 140930673, NIP: 701-00-65-944. Kapitał zakładowy: 200 000,00 PLN, w całości wpłacony.
Administrator Systemów Informatycznych	osoba wyznaczona przez Administratora Danych Osobowych, odpowiedzialna za funkcjonowanie i bezpieczeństwo systemów informatycznych

Dane niezidentyfikowane	Dane osobowe, których Administrator Danych Osobowych nie identyfikuje w odniesieniu do konkretnych podmiotów danych (np. zapis z monitoringu, korespondencja e-mailowa zawierająca dane osób trzecich)
Dane osobowe	wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; 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
Dane dzieci	dane osobowe osób fizycznych poniżej 16. roku życia
Dane karne	dane osobowe dotyczące wyroków skazujących i czynów zabronionych lub powiązanych środków bezpieczeństwa
Dane szczególne	dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych; dane genetyczne; dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej; dane dotyczące zdrowia, seksualności lub orientacji seksualnej osoby fizycznej
Dane zwykłe	dane osobowe, które nie są danymi szczególnymi
Dostępność	zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy, kiedy jest to potrzebne
Hasło	ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi
Identyfikator	ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym
Incydent	zdarzenie mogące wpłynąć na bezpieczeństwo danych osobowych w zakresie dostępności, integralności, poufności lub odporności systemów i usług przetwarzania. Incydent może prowadzić do naruszenia ochrony danych osobowych, ale nie musi
Inspektor Ochrony Danych (IOD)	osoba wyznaczona przez Administratora Danych Osobowych do wypełniania zadań przewidzianych w art. 39 ust. 1 RODO
Integralność	zapewnienie dokładności i kompletności informacji oraz metod przetwarzania

Naruszenie ochrony danych osobowych	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
Odbiorca danych osobowych	osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną (osobą) trzecią. Nie uznaje się za odbiorców organów publicznych, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii Europejskiej lub prawem państwa członkowskiego
Odporność	zdolność systemów informatycznych do prawidłowego funkcjonowania mimo dużego obciążenia
Osoba upoważniona	osoba upoważniona przez Administratora Danych Osobowych do przetwarzania danych osobowych w określonym przez niego zakresie
Państwo trzecie	państwo nienależące do Unii Europejskiej oraz Europejskiego Obszaru Gospodarczego
Podmiot danych	osoba fizyczna, której dane osobowe dotyczą
Podmiot przetwarzający	osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora Danych Osobowych
Polityka	niniejsza „Polityka ochrony danych osobowych w IT CONNECT Sp. z o.o.”
Poufność	zapewnienie, że dane osobowe są dostępne jedynie dla osób upoważnionych
Profilowanie	dowolna forma 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
Przetwarzanie danych osobowych	operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie

Pseudonimizacja	przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej
Raport	przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych
RODO	Rozporządzenie 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
Rozliczalność	wykazanie przez Administratora Danych Osobowych, że przestrzega przepisów dotyczących ochrony danych osobowych w prowadzonych procesach przetwarzania danych osobowych
Serwisant	firma lub pracownik firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego
Strona (osoba) trzecia	osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż: – osoba, której dane dotyczą; – Administrator Danych Osobowych i współadministrator danych osobowych; – podmiot przetwarzający; – osoba upoważniona
System informatyczny	zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych
System ochrony danych osobowych	całokształt środków technicznych, organizacyjnych i prawnych wraz z niezbędną dokumentacją, wdrożonych przez Administratora Danych Osobowych, służących zapewnieniu, że przetwarzanie danych osobowych będzie odbywało się zgodnie z przepisami z zakresu ochrony danych osobowych
Ustawa	Ustawa z dnia 29 sierpnia 1997 o ochronie danych osobowych
Uwierzytelnianie	działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu
Użytkownik	osoba upoważniona, której nadano identyfikator i przyznano hasło
Współadministrator danych osobowych	osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który wspólnie z Administratorem Danych Osobowych

	decyduje o celach i sposobach przetwarzania danych osobowych
Zagrożenie	potencjalna możliwość wystąpienia incydentu
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
Zgoda	dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych

II. FUNDAMENTY I ZASADY OCHRONY DANYCH OSOBOWYCH

§3.
Fundamenty systemu ochrony danych osobowych

1) Zarząd administratora danych, świadomy wagi zagrożeń jakie niesie ze sobą przetwarzanie danych osobowych dla wolności i praw osób, których dane dotyczą, uznaje ochronę tych danych, w szczególności zapewnienie ich bezpieczeństwa, za jeden z priorytetów działalności IT CONNECT Sp. z o.o. Podejmowane są działania mające na celu zapewnienie stałej zgodności działalności IT CONNECT Sp. z o.o. z tymi przepisami o ochronie danych osobowych. Zarząd administratora danych oczekuje, że zasady i procedury określone w niniejszym dokumencie będą faktycznie wdrożone i stosowane przez ich adresatów. Zobowiązuje się wszystkie osoby dopuszczone do przetwarzania danych osobowych w IT CONNECT Sp. z o.o. do dostosowania ich postępowania do wymogów wynikających z niniejszej *Polityki ochrony danych osobowych.*
2) Zasady i procedury określone w niniejszym dokumencie stosuje się zarówno do danych osobowych przetwarzanych w sposób tradycyjny w księgach, wykazach i innych zbiorach ewidencyjnych, jak i przetwarzanych w systemach informatycznych.
3) Zasady i procedury określone w niniejszym dokumencie stosuje się do wszystkich osób przetwarzających dane osobowe w ramach IT CONNECT Sp. z o.o., zarówno do zatrudnionych w IT CONNECT Sp. z o.o., jak i pozostałych, które zostały dopuszczone do przetwarzania, np. wolontariuszy, praktykantów, itd.

Administrator Danych Osobowych tworzy system ochrony danych osobowych w swojej organizacji, budując go na następujących fundamentach:

a) **podejście oparte na ryzyku** — Administrator Danych Osobowych jest zobowiązany zidentyfikować ryzyka towarzyszące przetwarzaniu danych osobowych oraz ustalić ich wpływ na operacje związane z danymi osobowymi, a w szczególności na prawa i wolności osób fizycznych;

b) **poszanowanie praw osób fizycznych** — Administrator Danych Osobowych, jak również wszystkie osoby zaangażowane w procesy przetwarzania danych osobowych, są zobowiązani ułatwić osobom fizycznym realizację ich praw związanych z ochroną danych osobowych;

c) **legalność** — Administrator Danych Osobowych, jak również wszystkie osoby zaangażowane w procesy przetwarzania danych osobowych, są zobowiązani przeprowadzać jakiekolwiek operacje związane z danymi osobowymi przy zachowaniu pełnej zgodności z obowiązującym prawem;

d) **bezpieczeństwo** — Administrator Danych Osobowych jest zobowiązany zapewnić bezpieczeństwo przetwarzania danych osobowych, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze;

e) **rozliczalność** — Administrator Danych Osobowych, jak również wszystkie osoby zaangażowane w procesy przetwarzania danych osobowych, są zobowiązani dokumentować sposób spełnienia obowiązków wynikających z przepisów z zakresu ochrony danych osobowych.

§4.

Zasady ochrony danych osobowych

Administrator Danych Osobowych przetwarza dane osobowe w oparciu o następujące zasady:
a) **zasada zgodności z prawem, rzetelności i przejrzystości** — dane osobowe są przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
b) **zasada ograniczenia celu** — dane osobowe są zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
c) **zasada minimalizacji danych** — dane osobowe są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;
d) **zasada prawidłowości** — dane osobowe są prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane;
e) **zasada czasowości** — dane osobowe są przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane;
f) **zasada integralności i poufności** — dane osobowe są przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

III. PODMIOTY TWORZĄCE SYSTEM OCHRONY DANYCH OSOBOWYCH

§5.

Administrator danych osobowych

Administrator danych osobowych realizuje zadania w zakresie ochrony danych osobowych, w tym zwłaszcza:

1) podejmuje decyzje o celach i środkach przetwarzania danych osobowych z uwzględnieniem zmian w obowiązującym prawie, organizacji administratora danych oraz technik zabezpieczenia danych osobowych;
2) upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi ich obowiązków;
3) wyznacza inspektora ochrony danych osobowych jako właściwego do prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych oraz pozostałej dokumentacji z zakresu ochrony danych, o ile jako właściwy do jej prowadzenia nie zostanie wskazany w niniejszym dokumencie inny podmiot;
4) zleca by zapewnione zostały użytkownikom odpowiednie stanowiska pracy umożliwiające bezpieczne przetwarzanie danych;
5) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych.

§6.

Administrator systemu

Administrator systemu realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym administratora danych, w tym zwłaszcza:

1) zarządza systemem informatycznym, w którym przetwarzane są dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych z pozycji administratora,
2) przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe,

3) na wniosek inspektora ochrony danych osobowych przydziela każdemu użytkownikowi identyfikator oraz hasło do systemu informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także usuwa konta użytkowników zgodnie z zasadami określonymi w instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
4) nadzoruje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych,
5) podejmuje działania w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego,
6) wyrejestrowuje użytkowników na wniosek administratora danych lub inspektora danych osobowych,
7) zmienia w poszczególnych stacjach roboczych hasła dostępu, ujawniając je wyłącznie danemu użytkownikowi oraz, w razie potrzeby administratorowi danych,
8) w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje inspektora ochrony danych osobowych o naruszeniu i współdziała z nim przy usuwaniu skutków naruszenia,
9) prowadzi szczegółową dokumentację naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym,
10) sprawuje nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe, nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego,
11) podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji.

§7.

Współadministrator danych osobowych

1. Administrator Danych Osobowych może wspólnie ustalać cele i sposoby przetwarzania danych osobowych ze współadministratorem danych osobowych — jeżeli taka konieczność wynika z przedsięwzięć realizowanych przez Administratora Danych Osobowych.
2. Administrator Danych Osobowych jest zobowiązany zawrzeć ze współadministratorem danych osobowych umowę o współadministrowanie danymi osobowymi.
3. W umowie o współadministrowanie danymi osobowymi należy określić w szczególności:
a) zakresy odpowiedzialności Administratora Danych Osobowych i współadministratora danych osobowych;
b) sposób realizowania obowiązków wynikających z przepisów z zakresu ochrony danych osobowych;
c) sposób spełnienia obowiązków informacyjnych z art. 13 RODO i art. 14 RODO;
d) punkt kontaktowy — jeżeli jest to wskazane;
e) relacje pomiędzy Administratorem Danych Osobowych i współadministratorem danych osobowych a podmiotami danych;
f) sposób przekazania podmiotom danych treści uzgodnień pomiędzy Administratorem Danych Osobowych a współadministratorem danych osobowych.

§8.

Inspektor Danych Osobowych

1. W przypadkach wskazanych w art. 37 ust. 1 RODO lub w prawie polskim Administrator Danych Osobowych jest zobowiązany wyznaczyć Inspektora Ochrony Danych.
2. W przypadkach innych niż wskazane w ust. 1, Administrator Danych Osobowych może podjąć decyzję o dobrowolnym wyznaczeniu Inspektora Ochrony Danych.
3. Administrator Danych Osobowych zawiadamia Prezesa Urzędu Ochrony Danych Osobowych w terminie 14 dni o:
a) wyznaczeniu Inspektora Ochrony Danych, podając jego dane kontaktowe;
b) zmianie Inspektora Ochrony Danych, podając jego dane kontaktowe;
c) rezygnacji z wyznaczania Inspektora Ochrony Danych, jeżeli wcześniej był wyznaczony.

4. Administrator Danych Osobowych może zatrudnić Inspektora Ochrony Danych na podstawie umowy o pracę lub na podstawie cywilnoprawnej umowy o świadczenie usług.
5. Z uwagi na konflikt interesów Inspektorem Ochrony Danych nie może być osoba zatrudniona na stanowisku, które decyduje o celach przetwarzania danych osobowych.
6. Inspektor Ochrony Danych ma za zadanie:
a) informować Administratora Danych Osobowych oraz osoby przez niego zatrudnione, które przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy prawa;
b) doradzać w sprawie przestrzegania przepisów z zakresu ochrony danych osobowych;
c) monitorować przestrzeganie przepisów z zakresu ochrony danych osobowych, niniejszej Polityki oraz innych dokumentów Administratora Danych Osobowych;
d) monitorować podział obowiązków;
e) podejmować działania zwiększające świadomość w zakresie ochrony danych osobowych;
f) przeprowadzać szkolenia osób zatrudnionych w zakresie ochrony danych osobowych;
g) prowadzić audyty;
h) udzielać na żądanie Administratora Danych Osobowych zaleceń co do oceny skutków dla ochrony danych osobowych oraz monitorować jej wykonanie zgodnie z art. 35 RODO;
i) współpracować z Prezesem Urzędu Ochrony Danych Osobowych;
j) pełnić funkcję punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzić konsultacje we wszelkich innych sprawach.
7. Administrator Danych Osobowych jest zobowiązany zapewnić, by Inspektor Ochrony Danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.
8. Administrator Danych Osobowych jest zobowiązany wspierać Inspektora Ochrony Danych w wypełnianiu przez niego zadań, o których mowa w ust. 7, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.

§9.

Osoby upoważnione

1.Przetwarzania danych osobowych w ramach struktury Administratora Danych Osobowych mogą dokonywać wyłącznie osoby upoważnione przez Administratora Danych Osobowych.
2. Administrator Danych Osobowych zapewnia, aby żadna z osób upoważnionych nie miała dostępu do większej ilości danych osobowych i procesów przetwarzania danych osobowych niż jest to konieczne do prawidłowego wypełniania obowiązków i zadań.
3. Procedura nadawania, zmiany i odbierania upoważnień stanowi **Załącznik nr 1.**
4. Osoba upoważniona do przetwarzania danych osobowych przed przystąpieniem do czynności ma obowiązek:
a) zapoznać się z dokumentami z zakresu ochrony danych osobowych, w szczególności z niniejszą Polityką — w zakresie ustalonym przez Administratora Danych Osobowych;
b) odbyć szkolenie z zakresu ochrony danych osobowych;
c) złożyć oświadczenie na piśmie o zapoznaniu się z dokumentami z zakresu ochrony danych osobowych oraz o odbyciu szkolenia z zakresu ochrony danych osobowych;
d) złożyć oświadczenie na piśmie o przestrzeganiu zasad ochrony danych osobowych oraz ustalonych procedur.
5. Wzory oświadczeń, o których mowa w ust. 4, stanowią **Załącznik nr 2.**
6. Oświadczenia, o których mowa w ust. 4, są dołączane do umowy zawartej z osobą upoważnioną lub do akt osobowych osoby upoważnionej.
7. Administrator Danych Osobowych zapewnia osobom upoważnionym dostęp do dokumentów z zakresu ochrony danych, z wyjątkiem tych dokumentów, które nie powinny być dostępne dla wszystkich osób upoważnionych.
8. Obowiązki określone w ust. 4 nie dotyczą osób, które są dopuszczane do przetwarzania danych osobowych incydentalnie (np. w celu naprawy sprzętu). W takiej sytuacji należy wskazać w treści zawartej umowy

obowiązek przestrzegania ochrony danych osobowych oraz przekazać najważniejsze informacje na temat ochrony danych osobowych. W zależności od sytuacji z takimi osobami można zawrzeć również umowę powierzenia.
9. Administrator Danych Osobowych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych.
10. Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych stanowi **Załącznik nr 3.**

§10.
Podmioty przetwarzające

1. Administrator Danych Osobowych może powierzyć przetwarzanie danych osobowych podmiotowi przetwarzającemu w zależności od własnych potrzeb.
2. Administrator Danych Osobowych jest zobowiązany powierzać przetwarzanie danych osobowych tylko takim podmiotom przetwarzającym, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. Zakazane jest korzystanie z usług podmiotów przetwarzających, które takich gwarancji nie dają.
3. Wzór umowy powierzenia przetwarzania danych osobowych stanowi **Załącznik nr 4.**
4. W przypadku korzystania przez podmiot przetwarzający z usług innego podmiotu przetwarzającego, który nie daje analogicznych gwarancji, o jakich mowa w ust. 2, Administrator Danych Osobowych jest zobowiązany wnieść sprzeciw, a w innych przypadkach — może wnieść sprzeciw, jeżeli istnieją ku niemu podstawy.
5. Administrator Danych Osobowych jest zobowiązany kontrolować przestrzeganie przez podmiot przetwarzający przepisów RODO przez cały okres trwania umowy.
6. W przypadku naruszania przez podmiot przetwarzający przepisów RODO Administrator Danych Osobowych jest zobowiązany niezwłocznie zaprzestać współpracy z podmiotem przetwarzającym.
7. Administrator Danych Osobowych prowadzi ewidencję podmiotów przetwarzających, z którymi zawarł umowy o powierzenie przetwarzania danych osobowych.
8. Wzór ewidencji podmiotów przetwarzających stanowi **Załącznik nr 5.**

§11.
Odbiorcy danych osobowych

1.Administrator Danych Osobowych ujawnia dane osobowe odbiorcom danych osobowych wyłącznie po zweryfikowaniu podstawy prawnej takiego ujawnienia.
2. W przypadku braku podstawy prawnej, o której mowa w ust. 1, Administrator Danych Osobowych odmawia ujawnienia danych osobowych jakiemukolwiek odbiorcy danych osobowych.
3. Administrator Danych Osobowych prowadzi ewidencję odbiorców danych osobowych – wzór stanowi **Załącznik nr 6**.
4. Administrator Danych Osobowych prowadzi rejestr żądań udostępnień danych osobowych – wzór stanowi **Załącznik nr 7**.

IV. PRZETWARZANIE DANYCH OSOBOWYCH

§12.
Zarządzanie ryzykiem

1. Administrator Danych Osobowych wdraża i utrzymuje procedurę zarządzania ryzykiem.
2. Administrator Danych Osobowych jest zobowiązany uwzględniać ryzyko w planowanych i prowadzonych procesach przetwarzania danych osobowych.
3. Procedura zarządzania ryzykiem stanowi **Załącznik nr 8**.

§13.

Ocena skutków dla ochrony danych osobowych

1. W przypadkach wskazanych w art. 35 ust. 1 RODO, art. 35 ust. 3 RODO oraz w odniesieniu do operacji przetwarzania znajdujących się w wykazie publikowanym przez Prezesa Urzędu Ochrony Danych Osobowych na podstawie art. 35 ust. 4 RODO Administrator Danych Osobowych jest zobowiązany przeprowadzić ocenę skutków dla ochrony danych osobowych.
2. Ocena skutków dla ochrony danych osobowych nie jest wymagana w odniesieniu do operacji przetwarzania znajdujących się w wykazie publikowanym przez Prezesa Urzędu Ochrony Danych Osobowych na podstawie art. 35 ust. 5 RODO.
3. Szablon oceny skutków dla ochrony danych osobowych stanowi **Załącznik nr 9.**

§14.

Uprzednie konsultacje z Prezesem Urzędu Ochrony Danych Osobowych

1. Jeżeli z oceny skutków dla ochrony danych osobowych wynika, że przetwarzanie powodowałoby wysokie ryzyko, gdyby Administrator Danych Osobowych nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania Administrator Danych Osobowych jest zobowiązany skonsultować się z Prezesem Urzędu Ochrony Danych Osobowych, zgodnie z wytycznymi w obowiązujących przepisach prawa.

§15.

Privacy by design i privacy by default

1. Administrator Danych Osobowych jest zobowiązany uwzględniać ochronę danych osobowych w fazie projektowania nowych systemów, programów, aplikacji, usług, a także w fazie projektowania nowych procesów i sposobów przetwarzania danych osobowych (privacy by design).
2. Administrator Danych Osobowych jest zobowiązany zapewnić domyślną ochronę danych osobowych, tj. domyślnie mogą być przetwarzane tylko te dane osobowe, które są niezbędne do osiągnięcia konkretnego celu przetwarzania (privacy by default).
Rezygnacja z prywatności lub jej ograniczenie mogą nastąpić tylko na wyraźne żądanie
podmiotu danych.
3. Procedura privacy by design i privacy by default stanowi **Załącznik nr 10**.

§16.

Infrastruktura przetwarzania danych

1. Administrator Danych Osobowych przetwarza dane osobowe na podstawie zgody tylko wówczas, gdy nie ma innej podstawy przetwarzania danych osobowych. Nie należy uzyskiwać zgody na przetwarzanie danych osobowych związanych z zawarciem i wykonaniem umowy lub w odniesieniu do takich danych osobowych, których obowiązek przetwarzania wynika z przepisów prawa.
2. Przed podjęciem decyzji o przetwarzaniu danych osobowych na podstawie zgody Administrator Danych Osobowych jest zobowiązany zweryfikować, czy dane osobowe są adekwatne do założonego celu przetwarzania.
3. Zabronione jest wywieranie przymusu w celu uzyskania.
4. Zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie je odróżnić od pozostałych kwestii.
5. Zgody muszą być formułowane w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.
7. Zgoda może być cofnięta w każdym momencie. Administrator Danych Osobowych zapewnia, aby wycofanie zgody było równie proste, jak jej złożenie.
8. Administrator Danych Osobowych jest zobowiązany zapewnić system zarządzania zgodami, który pozwoli zweryfikować, czy dana osoba udzieliła zgody na przetwarzanie danych osobowych, czy i kiedy ją wycofała.

§17.

Identyfikacja i weryfikacja podstaw prawnych przetwarzania danych

1. Administrator Danych Osobowych jest zobowiązany przetwarzać dane osobowe wyłącznie w oparciu o konkretną podstawę prawną.
2. Administrator Danych Osobowych jest zobowiązany w odniesieniu do każdej czynności przetwarzania danych osobowych zidentyfikować i zweryfikować podstawę prawną przetwarzania danych osobowych.
3. Administrator Danych Osobowych jest zobowiązany monitorować zmiany legislacyjne.
4. Administrator Danych Osobowych jest zobowiązany wskazać swoje prawnie uzasadnione interesy, legalizujące przetwarzanie danych osobowych na podstawie art. 6 ust. 1 lit. f RODO.
5. Osoby upoważnione do przetwarzania danych osobowych mają obowiązek znać podstawy prawne, w oparciu o które wykonują czynności związane z danymi osobowymi.
6. Przetwarzanie danych uzyskanych od podmiotów danych – **Załącznik nr 11a**.
7. Przetwarzanie danych uzyskanych od innego administratora – **Załącznik 11b**.

§18.

Minimalizacja danych

1. Administrator Danych Osobowych jest zobowiązany przestrzegać zasady minimalizacji.
2. W celu zapewnienia realizacji zasady minimalizacji Administrator Danych Osobowych w szczególności:

a) weryfikuje ilość przetwarzanych danych osobowych — Administrator Danych Osobowych nie może przetwarzać większej ilości danych osobowych niż to wynika z założonego celu;

b) weryfikuje zakres przetwarzanych danych osobowych — Administrator Danych Osobowych nie może podejmować większej liczby czynności przetwarzania niż to wynika z założonego celu;

c) ogranicza dostęp do danych osobowych poprzez stosowanie środków prawnych (umowy z klauzulami poufności, system upoważnień), środków fizycznych (kontrola dostępu osób do budynków, pomieszczeń i systemów) oraz środków logicznych (kontrola uprawnień w systemach informatycznych i dostępu do systemów informatycznych);

d) ogranicza czas przetwarzania danych osobowych — Administrator Danych Osobowych nie może przetwarzać danych osobowych dłużej niż to wynika z założonego celu.

3. Procedura usuwania i niszczenia danych osobowych stanowi **Załącznik nr 12**.

V. BEZPIECZEŃSTWO DANYCH OSOBOWYCH

Identyfikuje się następujące **zagrożenia bezpieczeństwa danych osobowych** przetwarzanych w IT CONNECT:

1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np. pożar, zalanie pomieszczeń, katastrofa budowlana, niepożądana ingerencja ekipy remontowej, włamanie do budynku;
2) niewłaściwe parametry środowiska, zakłócające pracę urządzeń komputerowych (nadmierna wilgotność lub bardzo wysoka temperatura, oddziaływanie pola elektromagnetycznego i inne);
3) awarie sprzętu lub oprogramowania, zarówno losowe, jak i spowodowane przez niewłaściwe działanie użytkowników i serwisantów,
4) zastosowanie niewłaściwych metod zabezpieczenia systemu informatycznego lub brak dostosowania poziomu zabezpieczeń do aktualnego poziomu wyzwań technologicznych;
5) działania przestępcze mające na celu przejęcie lub zniszczenie danych osobowych (np. ataki internetowe);
6) podejmowanie pracy w systemie z przełamaniem lub zaniechaniem stosowania procedur ochrony danych, np. praca osoby, która nie jest upoważniona do przetwarzania, pozostawienie serwisantów bez nadzoru, a także przyzwolenie na naprawę sprzętu zawierającego dane poza siedzibą administratora danych;
7) naruszenia zasad i procedur określonych w dokumentacji ochrony danych osobowych przez osoby upoważnione do przetwarzania danych osobowych, będące skutkiem nieprzestrzegania procedur ochrony danych, w tym zwłaszcza:

- wprowadzanie zmian do systemu informatycznego administratora danych i instalowanie programów bez wiedzy i zgody administratora systemu.
- ujawnienie osobom nieupoważnionym danych osobowych, jak też procedur ochrony danych stosowanych u administratora danych (poprzez umożliwienie wglądu lub przekazania danych i dokumentacji);
- naruszenie bezpieczeństwa danych przez nieautoryzowane ich przetwarzanie lub zgoda na takie działania przez inne osoby (np. udostępnienie identyfikatora i hasła innemu użytkownikowi);
- niezgodne z procedurami zakończenie pracy lub opuszczenie stanowiska pracy (nieprawidłowe wyłączenie komputera, niezablokowanie wyświetlenia treści pracy na ekranie komputera przed tymczasowym opuszczeniem stanowiska pracy, pozostawienie po zakończeniu pracy nieschowanych do zamykanych na klucz szaf dokumentów zawierających dane osobowe, niezamknięcie na klucz pokoju po jego opuszczeniu, nieoddanie klucza na portiernię), przetwarzanie danych osobowych w celach niezgodnych z ich przeznaczeniem,

Przeciwdziałanie zagrożeniom bezpieczeństwa danych osobowych:

Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych zawiera Załącznik nr 13.

1. Strefy bezpieczeństwa

1) W siedzibie administratora danych wydzielono strefę bezpieczeństwa, w której dostęp do informacji zabezpieczony jest środkami w postaci zamka cyfrowego na drzwiach (pomieszczenie z serwerem).
2) Do danych osobowych mają dostęp wszystkie osoby upoważnione do przetwarzania danych osobowych zgodnie z zakresami upoważnień do ich przetwarzania, a osoby postronne mogą w niej przebywać tylko w obecności pracownika upoważnionego do przetwarzania danych osobowych. Strefa ta obejmuje wszystkie pomieszczenia zaliczone do obszaru przetwarzania danych w siedzibie administratora danych.

2. Zabezpieczenie sprzętu

1) Serwer jest zlokalizowany w klimatyzowanym pomieszczeniu, zamykanym drzwiami z zamkiem cyfrowym.
2) Administrator systemu wskazuje użytkownikom, jak postępować, aby zapewnić prawidłową eksploatację urządzeń i systemu informatycznego;
3) Bieżąca konserwacja sprzętu administratora danych wykorzystywanego do przetwarzania danych osobowych prowadzona jest przez administratora systemu.
4) W przypadku konieczności dokonania naprawy przez podmiot zewnętrzny, w siedzibie administratora danych, dokonuje się tego po zawarciu z podmiotem wykonującym naprawę umowy o powierzenie przetwarzania danych osobowych lub po usunięciu tych danych.
5) W szczególnych przypadkach, gdy nie istnieje ryzyko naruszenia ochrony danych osobowych, można dokonać naprawy w warunkach określonych w ppkt. 6) bez zawarcia umowy o powierzeniu przetwarzania danych i bez usunięcia danych, jednak pod ścisłym nadzorem administratora systemu dbającego o to by serwisant nie miał dostępu do danych osobowych administratora danych.
6) Administrator systemu dopuszcza konserwowanie i naprawę sprzętu poza siedzibą administratora danych jedynie po trwałym usunięciu danych osobowych, a jeśli wiązałoby się to z nadmiernymi utrudnieniami, to po podpisaniu umów powierzenia przetwarzania danych osobowych.
7) Zużyty sprzęt służący do przetwarzania danych osobowych może być zbywany dopiero po trwałym usunięciu danych, a urządzenia uszkodzone mogą być przekazywane w celu utylizacji (jeśli trwałe usunięcie danych wymagałoby nadmiernych nakładów ze strony administratora) właściwym podmiotom, z którymi także zawiera się umowy powierzenia przetwarzania danych.

3. Zabezpieczenie systemu informatycznego

1) System informatyczny posiada szerokopasmowe połączenie z Internetem. Dostęp do niego jest jednak ograniczony.
2) Administrator danych wykorzystuje centralną zaporę sieciową w celu separacji lokalnej sieci od sieci publicznej.

3) Przed atakami z sieci zewnętrznej wszystkie komputery administratora danych (w tym także przenośne) chronione są środkami dobranymi przez administratora systemu. Ważne jest, by użytkownicy zwracali uwagę na to, czy urządzenie, na którym pracują, domaga się aktualizacji tych zabezpieczeń. O wszystkich takich przypadkach należy informować administratora systemu oraz umożliwić monitorowanie oraz aktualizację środków (urządzeń, programów) bezpieczeństwa.
4) Administrator systemu dobiera elektroniczne środki ochrony przed atakami z sieci stosownie do pojawiania się nowych zagrożeń (nowe wirusy, robaki, trojany, inne możliwości wdarcia się do systemu), a także stosownie do rozbudowy systemu informatycznego administratora danych i powiększania bazy danych. Jednocześnie należy zwracać uwagę, czy rozwijający się system zabezpieczeń sam nie wywołuje nowych zagrożeń.
Wszystkie awarie, działania konserwacyjne i naprawy systemu informatycznego są opisywane w stosownych protokołach, podpisywanych przez osoby w tych działaniach uczestniczące, a także przez administratora systemu.

4. Kontrola dostępu do systemu i monitorowanie pracy użytkowników

1) Poszczególnym osobom upoważnionym do przetwarzania danych osobowych przydziela się konta opatrzone niepowtarzalnym identyfikatorem, umożliwiające dostęp do danych, zgodnie z zakresem upoważnienia do ich przetwarzania. Administrator systemu lub z jego upoważnienia inny pracownik po uprzednim przedłożeniu upoważnienia do przetwarzania danych osobowych, zawierającego odpowiedni wniosek inspektora danych osobowych przydziela pracownikowi upoważnionemu do przetwarzania danych konto w systemie informatycznym, dostępne po wprowadzeniu prawidłowego identyfikatora i uwierzytelnieniu hasłem. System wymusza zmianę hasła przy pierwszym logowaniu.
2) W razie potrzeby, administrator systemu lub z jego upoważnienia inny może przydzielić konto opatrzone identyfikatorem osobie upoważnionej do przetwarzania danych osobowych, nieposiadającej statusu pracownika.
3) System informatyczny administratora danych zapewnia odnotowanie:
- daty pierwszego wprowadzenia danych do systemu,
- identyfikatora użytkownika wprowadzającego dane osobowe do systemu,
- źródła danych – w przypadku zbierania danych nie od osoby, której one dotyczą,
- informacji o odbiorcach danych, którym dane osobowe zostały udostępnione, o dacie i zakresie tego udostępnienia,
- wniesienia sprzeciwu wobec przetwarzania danych osobowych, o którym mowa w art. 21 RODO.
Odnotowanie daty pierwszego wprowadzenia danych do systemu oraz identyfikatora użytkownika następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.
4) Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ppkt 3).
5) Administrator systemu przeprowadza synchronizację zegarów stacji roboczych z serwerem, ograniczając dopuszczalność zmian w ustawieniach zegarów. Jakiekolwiek zmiany ustawień zegarów mogą być dokonywane jedynie przez administratora systemu z konta o uprawnieniach administracyjnych.
6) System informatyczny administratora danych umożliwia zapisywanie zdarzeń wyjątkowych na potrzeby audytu i przechowywanie informacji o nich przez określony czas. Zapisy takie obejmują:
- identyfikator użytkownika,
- datę i czas zalogowania i wylogowania się z systemu,
- tożsamość stacji roboczej,
- zapisy udanych i nieudanych prób dostępu do systemu,
- zapisy udanych i nieudanych prób dostępu do danych osobowych i innych zasobów systemowych.

5. Polityka osobowa

1) Nabór pracowników na stanowiska związane z przetwarzaniem danych osobowych dokonywany jest z uwzględnieniem kompetencji merytorycznych oraz postawy etycznej u kandydatów. Zwraca się uwagę na takie cechy kandydata, jak uczciwość, odpowiedzialność i przewidywalność zachowań.

2) Dopuszczenie do stanowisk związanych z przetwarzaniem danych osobowych następuje po zrealizowaniu obowiązków wynikających z przepisów prawa oraz niniejszej *Polityki ochrony danych osobowych*, w szczególności po wystawieniu stosownego indywidualnego upoważnienia oraz zapoznaniu osób dopuszczanych do przetwarzania z zasadami dotyczącymi bezpieczeństwa danych osobowych.
3) Ryzyko naruszenia zasad ochrony danych osobowy ze strony osób, które nie zostały upoważnione do przetwarzania danych osobowych (np. personel sprzątający) jest minimalizowane przez odpowiednie przeszkolenie ich (pouczenie) oraz zobowiązywanie do zachowania tajemnicy.

6. Indywidualne wymagania dotyczące użytkowników

Użytkownicy zobowiązani są do zachowania następujących reguł bezpieczeństwa:

1) powstrzymywania się od samodzielnej ingerencji w oprogramowanie i konfigurację powierzonego sprzętu oraz instalowania nieautoryzowanego oprogramowania, nawet gdy z pozoru mogłoby to usprawnić pracę lub podnieść poziom bezpieczeństwa danych;
2) dbania o prawidłową wentylację komputerów (nie można zasłaniać kratek wentylatorów meblami, zasłonami lub stawiać komputerów tuż przy ścianie);
3) niepodłączania do listew podtrzymujących napięcie przeznaczonych dla sprzętu komputerowego innych urządzeń, szczególnie tych łatwo powodujących spięcia (np. grzejniki, czajniki, wentylatory);
4) zamykania okien w razie opadów czy innych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych osobowych;
5) przestrzegania indywidualnych uprawnień i realizacji obowiązków w zakresie przetwarzania danych osobowych, w szczególności właściwego korzystania z powierzonych sprzętów i udostępnionych zasobów oraz używania wyłącznie własnego identyfikatora i hasła;
6) odpowiedniego zabezpieczenia identyfikatora i hasła wymaganego do uwierzytelnienia się w systemie oraz nieudostępniania go innym osobom;
7) zachowania danych osobowych i sposobu ich zabezpieczenia w tajemnicy, w tym także wobec osób najbliższych;
8) ustawiania ekranów komputerowych tak, by osoby nieuprawnione nie widziały treści wyświetlanych na ekranie;
9) niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych;
10) niepozostawiania bez kontroli włączonych urządzeń zawierających dane osobowe oraz niezabezpieczonych dokumentów (czasowe opuszczania stanowiska pracy jest dopuszczalne dopiero po aktywizowaniu wygaszacza ekranu lub po zablokowaniu urządzenia w inny sposób);
11) niszczenia niepotrzebnych wydruków i kopii dokumentów po ich wykorzystaniu oraz kasowania po wykorzystaniu danych z dysków przenośnych;
12) przekazywania danych osobowych pocztą elektroniczną z zachowaniem wszelkich środków ostrożności;
13) zapisywanie plików lub wykonywania kopii roboczych danych, na których się właśnie pracuje, tak często jak to możliwe, aby zapobiec ich utracie;
14) kończenia pracy na stacji roboczej po wprowadzeniu danych przetwarzanych tego dnia w odpowiednie obszary serwera, a następnie prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera
15) zadbanie o odpowiednie zabezpieczenie wszelkich dokumentów i wydruków zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy (np. w szafie zamykanej na klucz);
16) umieszczania kluczy do szaf w ustalonym, przeznaczonym do tego miejscu po zakończeniu dnia pracy;
17) zamykania drzwi na klucz po zakończeniu pracy w danym dniu.

7. Komputery przenośne i praca poza siedzibą administratora

1) Wynoszenie poza obszar przetwarzania danych urządzeń i dokumentów zawierających dane osobowe jest dopuszczalne jedynie za wiedzą i zgodą administratora systemu lub bezpośredniego przełożonego;.
2) Urządzenia zawierające dane osobowe wynoszone poza obszar przetwarzania danych należy chronić przed uszkodzeniami fizycznymi. Należy też bezwzględnie przestrzegać zaleceń producentów dotyczących ochrony sprzętu. W szczególności należy pamiętać, że urządzenia elektroniczne mogą ulec uszkodzeniu w skutek

działanie silnego pola elektromagnetycznego i chronić je przed takim oddziaływaniem.

3) Urządzenia przenośne, nośniki danych oraz dokumenty wynoszone poza obszar przetwarzania danych nie powinny być pozostawiane bez nadzoru. W szczególności zabrania się pozostawiania urządzeń i dokumentów zawierających dane osobowe bez odpowiedniego zabezpieczenia w miejscach publicznych, pokojach hotelowych oraz w samochodach.
4) Wykorzystywanie urządzeń przenośnych, nośników danych oraz dokumentów zawierających dane osobowe w miejscach publicznych jest dozwolone, o ile otoczenie, w którym znajduje się osoba upoważniona do przetwarzania danych osobowych, stwarza warunki minimalizujące ryzyko utraty, zniszczenia lub zapoznania się z danymi przez osoby nieupoważnione. Za miejsca szczególnego ryzyka należy uznać restauracje oraz środki komunikacji publicznej.
5) Niedozwolone jest udostępnianie urządzeń przenośnych i nośników danych należących do administratora danych osobom nieupoważnionym, w tym domownikom i osobom bliskim użytkownika. Użytkownik obowiązany jest zachować w tajemnicy wobec wszystkich osób, w tym wobec domowników i osób bliskich identyfikator i hasło, których podanie jest konieczne do rozpoczęcia pracy na komputerze przenośnym administratora danych lub chroniącym dostęp do nośników danych.
6) Administrator systemu w razie potrzeby wskazuje w dokumencie powierzenia komputera przenośnego osobie upoważnionej do przetwarzania danych osobowych konieczność i częstotliwość sporządzania kopii zapasowych danych przetwarzanych na komputerze przenośnym oraz określa termin i zasady zwrotu sprzętu.

VI. KOMUNIKACJA, INFORMACJE

1. Realizacja obowiązków informacyjnych i zapewnienie przejrzystej komunikacji

1. Administrator Danych Osobowych jest zobowiązany realizować obowiązki informacyjne, o których mowa w art. 13 RODO i art. 14 RODO.

2. Administrator Danych Osobowych spełnia obowiązek informacyjny:

a) w przypadku pozyskania danych bezpośrednio od podmiotu danych — w chwili pozyskiwania tych danych;

b) w przypadku pozyskiwania danych osobowych nie od podmiotu danych:

— w rozsądnym terminie po pozyskaniu danych, jednak nie później niż w terminie miesiąca;

— najpóźniej przy pierwszej komunikacji z podmiotem danych, jeżeli dane osobowe mają być wykorzystywane do komunikacji;

— przy pierwszym ujawnieniu, jeżeli dane osobowe mają być ujawnione innemu odbiorcy.

3. Administrator Danych Osobowych nie jest zobowiązany zrealizować obowiązku informacyjnego w przypadku pozyskiwania danych od podmiotu danych, gdy podmiot danych już posiada te informacje.

4. Administrator Danych Osobowych nie jest zobowiązany zrealizować obowiązku informacyjnego w przypadku pozyskiwania danych nie od podmiotu danych, gdy:

a) podmiot danych dysponuje już tymi informacjami;

b) udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku, w szczególności w przypadku przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem warunków i zabezpieczeń, o których mowa w art. 89 ust. 1 RODO, lub o ile wykonanie obowiązku informacyjnego może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania. W takich przypadkach Administrator Danych Osobowych podejmuje odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy podmiotu danych, w tym udostępnia informacje publicznie;

c) pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii Europejskiej lub prawem polskim; lub

d) dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii Europejskiej lub w prawie polskim, w tym ustawowym obowiązkiem zachowania tajemnicy.

5. Administrator Danych Osobowych informuje podmiot danych o planowanej zmianie celu przetwarzania danych osobowych.

6. Administrator Danych Osobowych informuje podmiot danych o planowanym uchyleniu ograniczenia

przetwarzania danych osobowych.
7. Administrator Danych Osobowych udziela informacji w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.
8. Administrator Danych Osobowych jest zobowiązany opracować zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.

2. Rodzaje uprawnień osób fizycznych

Oprócz prawa do informacji, o których mowa w § 22, każdemu podmiotowi danych przysługuje prawo do:
a) dostępu do danych osobowych i informacji o nich;
b) uzyskania kopii jego danych osobowych;
c) sprostowania danych osobowych i uzupełnienia niekompletnych danych osobowych;
d) usunięcia danych osobowych (prawo do bycia zapomnianym);
e) ograniczenia przetwarzania danych osobowych;
f) uzyskania informacji o odbiorcach danych osobowych w przypadku sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych;
g) uzyskania danych osobowych w określonym formacie i przesłania ich innemu administratorowi danych osobowych;
h) żądania przesłania danych osobowych innemu administratorowi danych osobowych przez Administratora Danych Osobowych;
i) wyrażenia sprzeciwu wobec przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. e RODO i art. 6 ust. 1 lit. f RODO, w tym profilowania;
j) wyrażenia sprzeciwu wobec marketingu bezpośredniego, w tym profilowania;
k) niepodlegania decyzji, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu.

3. Realizacja żądań osób, których dane dotyczą

1) Jeżeli zainteresowany skorzysta z prawa dostępu do danych (zażąda informacji na temat dotyczącego go przetwarzania) to udziela się mu jej zgodnie z art. 12 ust. 1 i 2 RODO. Jeśli podmiot danych tego zażąda, a jest to możliwe, przekazuje się mu także kopię dotyczących go danych. Informacji na żądanie udziela się zasadniczo w terminie miesiąc, chyba, że sprawa jest skomplikowana. Wtedy przedłużenie terminu następuje zgodni z art. 12 ust. 3 RODO.
2) Jeżeli zainteresowany skorzysta z prawa do sprostowania to na jego żądanie dokonuje się sprostowania nieprawidłowych danych. Prawo to obejmuje też uzupełnienie niekompletnych danych, przy czym kompletność ocenia się z uwzględnieniem celów przetwarzania. O ile to możliwe to o dokonanym sprostowaniu informuje się odbiorców, którym dane zostały przekazane.
3) Jeżeli zainteresowany skorzysta z prawa do usunięcia danych (bycia zapomnianym) to na jego żądanie usuwa się dotyczące go dane, chyba że spełnione są wymogi ich dalszego przetwarzania z art. 17 ust. 3 RODO. O ile to możliwe to o dokonanym usunięciu informuje się odbiorców, którym dane zostały przekazane. Gdy dane zostały upublicznione należy podjąć starania w celu usunięcia wszelkich łączy do tych danych, ich kopii lub replikacji stworzonych przez innych administratorów.
4) Jeżeli zainteresowany skorzysta z prawa do ograniczenia przetwarzania to na jego żądanie należy ograniczyć przetwarzanie do wskazanych czynności, chyba, że zachodzą przesłanki ich dalszego przetwarzania, w szczególności te wymienione w art. 18 ust. 2 RODO. O ile to możliwe to o dokonanym ograniczeniu informuje się odbiorców, którym dane zostały przekazane.
5) Jeżeli zainteresowany skorzysta z prawa do przeniesienia danych to dostarcza mu się dotyczących go danych w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego. Prawo to przysługuje, gdy dane mają postać zapisu elektronicznego i są przetwarzane na podstawie warunku zgody lub realizacji umowy. Na żądanie zainteresowanego dane dostarcza się bezpośrednio wskazanemu przez niego podmiotowi.
6) Jeżeli zainteresowany skorzysta z prawa sprzeciwu wobec przetwarzania jego danych osobowych, w tym profilowania, powołując się na swoją szczególną sytuację, to należy zaprzestać dalszego przetwarzania dotyczących go danych, chyba, że spełnione są przesłanki dalszego przetwarzania określone w art. 21 ust. 1

RODO.

7) Jeżeli zainteresowany skorzysta z prawa sprzeciwu wobec przetwarzania jego danych w celach marketingowych, w tym profilowania, to nie można nie uwzględnić sprzeciwu.
8) Procedura obsługi żądań podmiotów danych zawiera **Załącznik nr 14**.

4. Zgoda na przetwarzanie danych osobowych

1) Jeżeli zgodnie z art. 6 ust. 1 lub 9 ust. 1 RODO podstawą przetwarzania danych osobowych jest zgoda osoby, której dane dotyczą to przyzwolenie na przetwarzanie danych powinno być dobrowolne, konkretne, świadome i jednoznaczne. Musi spełniać też wymogi rozliczalności i transparentności.
2) Zapewnia się prawo do wycofania zgody.
3) Nie jest dopuszczalne uzależnienie wykonania usługi niezwiązanej bezpośrednio ze zgodą od jej udzielenia.
4) W przypadku usług społeczeństwa informacyjnego oferowanych dziecku podejmuje się wszelkie niezbędne działania by uzyskać aprobatę opiekuna.
5) Treść klauzuli informacyjnej zawiera **Załącznik nr 15.**

5. **Profilowanie**

1) Podejmowanie zautomatyzowanych decyzji wobec indywidualnych osób, w tym profilowanie, jest dopuszczalne wyłącznie w przypadkach określonych w art. 22 ust. 3, w szczególności, gdy zainteresowana osoba wyraziła na to zgodę.
2) Osobie, wobec której są podejmowane zautomatyzowane decyzje lub którą się profiluje zapewnia się:
   - prawo do zakwestionowania tej decyzji;
   - prawo do wyrażenia własnego stanowiska w przedmiocie podejmowanych wobec niej działań;
   - prawo do indywidualnego rozpatrzenia jej sprawy przez administratora danych;
   - prawo do wniesienia sprzeciwu zgodnie z art. 21 ust. 1 i 2 RODO.

6. **Udostępnianie danych osobowych**

1) Jeśli zgodnie z przepisami prawa administrator danych jest zobowiązany do przekazywana danych osobowych wskazanym podmiotom (np. Urzędowi Skarbowemu lub ZUS) to upoważnieni pracownicy administratora danych realizują ten wymóg zgodnie z zakresem swoich obowiązków służbowych stosując się ściśle do wskazanych przepisów.
2) Jeśli do administratora danych wystąpi z wnioskiem o udzielenie informacji osobowej podmiot, który twierdzi, że jest uprawniony do uzyskania takiej informacji na podstawie przepisów prawa udostępnienie informacji może nastąpić jedynie po:
   - zweryfikowaniu podstawy prawnej udostępnienia;
   - zweryfikowaniu czy składający wniosek jest podmiotem za który się podaje;
   - odnotowaniu udostępnienia w ewidencji udostępnień danych osobowych.

   Ewidencję udostępnień danych osobowych prowadzi Specjalista ds. kadr.
3) W przypadku, gdy z wnioskiem o którym mowa w ppkt. 2) wystąpi uprawniony funkcjonariusz, w szczególności policji, i wnioskujący stwierdzi, że istnieje konieczność niezwłocznego działania udostępnienie informacji może nastąpić po:
   - wylegitymowaniu funkcjonariusza;
   - na podstawie pisemnego oświadczenia funkcjonariusza lub za pisemnym pokwitowaniem przez niego uzyskania dokumentów.

   Jeśli złożenie oświadczenia lub pokwitowanie uzyskania danych przez funkcjonariusza nie są możliwe ze względu na okoliczności udostępniania, osoba udostępniająca informacje sporządza na tę okoliczność notatkę służbową. Ewidencjonując udostępnienie Specjalista ds. kadr opisze w rubryce „Uwagi" ewidencji udostępnień szczególne okoliczności udostępnienia.
4) Jeśli do administratora danych wystąpi z wnioskiem o udzielenie informacji osobowej podmiot, który nie jest uprawniony do uzyskania takiej informacji na podstawie przepisów prawa udostępnienie informacji może nastąpić jedynie gdy:
   - cel przetwarzania nie ulega zmianie;

- osobie, której dane mają być udostępnione zostanie umożliwione skorzystanie z prawa sprzeciwu;
- nastąpi zweryfikowanie tożsamości podmiotu składającego wniosek;
- udostępnienie zostanie odnotowane w ewidencji udostępnień danych osobowych.

7. **Przekazywanie danych do państw trzecich lub organizacji międzynarodowym**

1) Przekazywanie danych osobowych do państw trzecich jest zasadniczo zabroniona, chyba, że decyzję taką podejmie administrator danych, ze względu na szczególne okoliczności.
2) W przypadku określonym w ppkt. 1) przekazanie jest dokonywane wyłącznie zgodnie z wymogami określonymi w art. 44-50 RODO. Administrator danych dokłada staranności, by zapewnić stopień ochrony osób fizycznych zagwarantowany w RODO.

8. **Współpraca z podmiotami przetwarzającymi**

1) Jeśli wymagają tego okoliczności administrator danych może podjąć decyzje o powierzeniu przetwarzania danych osobowych podmiotowi przetwarzającemu.
2) Wybierając podmiot przetwarzający administrator danych dokłada staranności, by podmiot ten zapewniał wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO.
3) Powierzenie danych osobowych podmiotowi przetwarzającemu następuje na podstawie pisemnej umowy określającej przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych, kategorie osób, których dane dotyczą, a także obowiązki i prawa administratora danych i podmiotu przetwarzającego.
4) Umowa o której mowa w ppkt. 3) zawiera w szczególności:

a. zobowiązanie przetwarzającego do tego, że przetwarzanie danych osobowych będzie się odbywało wyłącznie na udokumentowane polecenie administratora danych,
b. deklarację przetwarzającego, że osoby upoważnione przez niego do przetwarzania danych osobowych zobowiązały się lub zobowiążą do zachowania w tajemnicy dane osobowe oraz sposób ich zabezpieczenia;
c. deklarację przetwarzającego, że wdrożył lub wdroży odpowiednie środki techniczne i organizacyjne, aby zapewnić odpowiedni stopień bezpieczeństwa zgodnie z art. 32 RODO,
d. deklarację przetwarzającego wskazującą, że jeśli korzysta lub będzie korzystać z usług innego podmiotu przetwarzającego, to wypełnia lub wypełni warunki określone w art. 28 ust. 2 i 4 RODO,
e. zobowiązanie przetwarzającego do pomocy administratorowi danych poprzez odpowiednie środki techniczne i organizacyjne w wywiązaniu się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w pkt. 1-7,
f. zobowiązanie przetwarzającego do pomocy administratorowi danych w realizacji określonych obowiązków;
g. zobowiązanie przetwarzającego do usunięcia lub zwrotu wszelkich danych osobowych administratora oraz wszelkich ich istniejących kopii po zakończeniu świadczenia usług, jeśli administrator danych wystąpi z takim żądaniem.

5) Umowy z podmiotami przetwarzającymi są przekazywane koordynatorowi procesów biznesowych w celu włączenia do dokumentacji ochrony danych osobowych.

9. Współadministrowanie

1) Jeśli wymagają tego okoliczności administrator danych może podjąć decyzje o wspólnym ustaleniu celów i sposobów przetwarzania danych osobowych z innym administratorem (tzw. współadministrowanie).
2) Uzgodnienie wskazane w ppkt. 1) jest zawierane w formie umowy pisemnej.
3) Umowa o której mowa w ppkt. 2) w przejrzysty sposób:

a. określa odpowiednie zakresy odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO, w szczególności obowiązków informacyjnych oraz innych obowiązków względem osób, których dane dotyczą,
b. wskazuje jak osoby, których dane dotyczą mogą kontaktować się w celu uzyskania informacji i realizacji przysługujących im praw.

4) Umowa o której mowa w ppkt. 1) w zakresie w jakim dotyczy osób, których dane mają być przetwarzane jest

udostępniana tym osobom na ich żądanie.

VII. DZIAŁANIA NADZORCZE I AUDYTY

1. Nadzór nad przestrzeganiem ochrony danych osobowych

1) W celu zapewnienia ochrony wolności i praw osób, których dane dotyczą, a zwłaszcza bezpieczeństwa dotyczących ich danych, administrator danych zapewnia zgodność działalności IT CONNECT Sp. z o.o. z przepisami.
2) Realizując zadanie określone w ppkt. 1) administrator danych lub osoba przez niego wskazana, w szczególności:

a. dokonuje inwentaryzacji zasobów danych osobowych i dba o aktualność ich opisu
b. przeprowadza ocenę ryzyka naruszenia ochrony danych osobowych
c. jeśli to wymagane prowadzi rejestr czynności przetwarzania
d. jeśli to wymagane przeprowadza ocenę skutków dla ochrony danych
e. jeśli to wymagane prowadzi uprzednie konsultacje z organem nadzorczym
f. czuwa nad aktualnością dokumentacji z zakresu ochrony danych osobowych
g. czuwa nad przestrzeganiem zasad określonych w dokumentacji ochrony danych osobowych
h. czuwa nad zgodnością przetwarzania danych osobowych z przepisami o ochronie danych osobowych
i. prowadzi postępowanie wyjaśniające w przypadku stwierdzenia naruszenia lub podejrzenia naruszenia ochrony danych osobowych

3) W celu realizacji zadań określonych w ppkt. 2 lit. f-h) przeprowadzane są okresowe audyty wewnętrzne (tzw. sprawdzenia planowe). Realizując zadanie określone w ppkt. 2 lit. i przeprowadzany jest audyt wewnętrzny nieobjęty planem sprawdzeń (tzw. sprawdzenie doraźne).
4) Administrator danych zapewnia (nadzoruje) realizację obowiązku zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie tych danych, w szczególności decyduje o terminach i sposobach przeprowadzenia szkoleń w tym zakresie.

2. Inwentaryzacja i opis zasobów

1) Inspektor ochrony danych osobowych dba o to by przetwarzanie danych osobowych w IT CONNECT Sp. z o.o odbywało się wyłącznie za wiedzą, zgodą i pod nadzorem osób upoważnionych. W celu realizacji tego zadania inspektor ochrony danych osobowych opisuje zasoby danych osobowych oraz sposób ich przetwarzania i zabezpieczenia zgodnie z załącznikiem Opis zasobów danych osobowych.
2) Inspektor ochrony danych osobowych dba o aktualność opisu zasobów.

3. Rejestr czynności przetwarzania

1) Administrator Danych Osobowych prowadzi i aktualizuje rejestr czynności przetwarzania danych osobowych, który jest najważniejszym dokumentem w zakresie ochrony danych osobowych.
2) Rejestr czynności przetwarzania danych osobowych służy:
   a) inwentaryzowaniu i monitorowaniu sposobu przetwarzania danych osobowych;
   b) dokumentowaniu czynności przetwarzania danych osobowych;
   c) wykazaniu realizacji zasady rozliczalności.

4. Audyty wewnętrzne

1) W celu zapewnienia przestrzegania przepisów o ochronie danych osobowych inspektor ochrony danych

osobowych przeprowadza następujące audyty wewnętrzne:
- sprawdzenie prawidłowości i aktualności dokumentacji z zakresu ochrony danych osobowych;
- sprawdzenie przestrzegania zasad i procedur określonych w dokumentacji ochrony danych osobowych.
- sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych;

2) Audyty wewnętrzne przeprowadzane są okresowo zgodnie z planem sprawdzeń przygotowywanym przez inspektora ochrony danych osobowych (sprawdzenia planowe). Plan sprawdzeń obejmuje maksimum 1 rok. Jest on przekazywany administratorowi danych do wiadomości w terminie minimum 2 tygodni przed rozpoczęciem okresu, który plan obejmuje. Jeśli sprawdzenie planowe obejmuje kontrolę w konkretnej jednostce lub dziale to kierownik tej jednostki jest zawiadamiany o sprawdzeniu nie później niż na 7 dni przed rozpoczęciem sprawdzenia.
3) W sytuacji powzięcia wiadomości o naruszeniu ochrony danych osobowych lub uzasadnionego podejrzenia wystąpienia takiego naruszenia inspektor ochrony danych osobowych przeprowadza audyt nieobjęty planem sprawdzeń (tzw. sprawdzenie doraźne). W przypadku sprawdzeń doraźnych terminy określone w ppkt. 2) nie obowiązują.
4) Inspektor ochrony danych osobowych przygotowuje i gromadzi dokumentację przeprowadzonych audytów.
5) Obowiązki określone w ppkt. 1-4) inspektor ochrony danych osobowych realizuje we współpracy z administratorem systemu posługując się w razie potrzeby pracownikami działu rekrutacji oraz działu kadr.
6) Kartę audytu wewnętrznego zawiera **Załącznik nr 16**.
7) Procedurę audytu wewnętrznego zawiera **Załącznik nr 17**.
8) Projekt planu audytu zawiera **Załącznik nr 18**.

5. Zapewnienie aktualności dokumentacji z zakresu ochrony danych osobowych

1) Inspektor ochrony danych osobowych dokłada starań by dokumentacja ochrony danych osobowych była aktualna. W tym celu na bieżąco śledzić zmiany stanu prawnego oraz zapoznaje się z treścią wytycznych i wskazówek wydawanych przez organ nadzorczy w tym zakresie.
2) Niezależnie od działań wskazanych w ppkt. 1) inspektor ochrony danych osobowych nie rzadziej niż raz do roku dokonuje przeglądu dokumentacji pod kątem sprawdzenia jej aktualności i zgodności z przepisami.

6. Zapewnienie przestrzegania zasad określonych w dokumentacji ochrony danych osobowych.

1) Inspektor ochrony danych osobowych prowadzi bieżący nadzór nad działalnością IT CONNECT Sp. z o.o**,** związaną z przetwarzaniem danych osobowych. Realizując powyższe zadanie inspektor ochrony danych osobowych m.in. na bieżąco ocenia zagrożenia, sprawdza kluczowe punkty bezpieczeństwa, formułuje zalecenia i wskazówki, odpowiada na pytania i udziela porad.
2) Niezależnie od działań wskazanych w ppkt. 1) inspektor ochrony danych osobowych nie rzadziej niż raz do roku przeprowadza audyt przestrzegania zasad i procedur ochrony danych osobowych w IT CONNECT Sp. z o.o.
3) W ramach audytu określonego w ppkt. 2) dokonuje się w szczególności analizy zagrożeń określonych w części IV niniejszej *Polityki* oraz sprawdza realizację wskazań i obowiązków określonych w części V niniejszej *Polityki*.

7. Obowiązek zapewnienia bezpieczeństwa przetwarzania danych osobowych

1. Administrator Danych Osobowych wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku przetwarzania danych osobowych.
2. Dobór odpowiednich środków technicznych i organizacyjnych następuje w ramach procedury zarządzania ryzykiem oraz ewentualnie w oparciu o ocenę skutków dla ochrony danych osobowych.
3. Dobór odpowiednich środków technicznych i organizacyjnych następuje z uwzględnieniem:
a) stanu wiedzy technicznej;
b) kosztów wdrażania;
c) charakteru, zakresu, kontekstu i celów przetwarzania;
d) ryzyka naruszenia praw i wolności osób fizycznych.

8. Systemy informatyczne

1. Administrator Danych Osobowych — jeżeli zajdzie taka potrzeba — może wyznaczyć Administratora Systemów Informatycznych. Jeżeli takiej osoby nie wyznacza, Administrator Danych Osobowych samodzielnie zarządza systemami informatycznymi.
2. Zasady związane z obsługą systemów informatycznych oraz ich zabezpieczeniem określa Instrukcja zarządzania systemami informatycznymi.
3. Instrukcja zarządzania systemami informatycznymi zawiera **Załącznik nr 19**.
4. Instrukcja, o której mowa w ust. 3, nie jest udostępniana ogółowi osób upoważnionych. Administrator Danych Osobowych określa, jakie osoby mogą uzyskać wgląd w treść Instrukcji, o której mowa w ust. 3.

9. Kontrola przetwarzania danych osobowych

Przynajmniej raz na rok Administrator Danych Osobowych / Inspektor Ochrony Danych / dokonuje przeglądu:
a) ilości przetwarzanych danych osobowych;
b) procesów przetwarzania danych osobowych;
c) upoważnień do przetwarzania danych osobowych;
d) użytkowników w systemach informatycznych.
2. W zakresie wynikającym z przeglądu, o którym mowa w ust. 1, dokonuje się niezbędnych usunięć i aktualizacji, aby zapewnić zgodność z niniejszą Polityką.

10. Szkolenia

1. Administrator Danych Osobowych jest zobowiązany podejmować działania na rzecz zwiększenia świadomości z zakresu ochrony danych osobowych wśród osób przez siebie zatrudnionych oraz podnoszenia ich wiedzy i kwalifikacji w tym zakresie.
2. Administrator Danych Osobowych zapewnia osobom przez siebie zatrudnionym szkolenia z zakresu ochrony danych osobowych, których częstotliwość oraz stopień zaawansowania zależy od pozycji zatrudnionego w systemie ochrony danych osobowych.
3. Wzór karty szkolenia zawiera **Załącznik nr 20**.
4. Wzór testu zawiera **Załącznik nr 21.**

VIII. NARUSZENIE OCHRONY DANYCH OSOBOWYCH

1. Postępowanie w przypadku stwierdzenia lub podejrzenia stwierdzenia naruszenia ochrony danych osobowych

1) Zasady postępowania w przypadku stwierdzenia naruszenia lub podejrzenia naruszenia bezpieczeństwa systemu informatycznego określa *Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w* IT CONNECT Sp. z o.o,
2) Każdy kto stwierdził inne niż określone w ppkt. 1) naruszenie ochrony danych osobowych lub podejrzewa takie naruszenie powinien niezwłocznie poinformować o tym inspektora ochrony danych osobowych. Jako inne niż określone w ppkt. 1) naruszenie rozumie się w szczególności brak realizacji lub niewłaściwą realizację wymogów określonych w części VI niniejszej *Polityki*.
3) Inspektor ochrony danych osobowych po otrzymaniu zawiadomienia, o którym mowa w ppkt. 2) przeprowadza niezwłocznie postępowanie wyjaśniające w celu ustalenia czy naruszenie ochrony danych osobowych miało miejsce (tzw. sprawdzenie doraźne).
4) Sprawdzenie doraźne może zostać wszczęte przez inspektora ochrony danych osobowych także z własnej inicjatywy, gdy w inny sposób niż w skutek zawiadomienia poweźmie informację o naruszeniu lub możliwym naruszeniu ochrony danych osobowych.
5) W przypadku stwierdzenia naruszenia ochrony danych osobowych w trybie określonym w ppkt. 3 inspektor ochrony danych osobowych:

a. w porozumieniu z odpowiednim kierownikiem podejmuje niezwłoczne, możliwe do wprowadzenia na bieżąco, działania zapobiegające dalszemu naruszaniu ochrony danych osobowych,
b. w porozumieniu z odpowiednim kierownikiem stosuje niezwłoczne, możliwe do wprowadzenia na bieżąco,

środki eliminujące lub zmniejszające ryzyko naruszenia praw lub wolności osoby, której dane dotyczą,

c. sporządza raport naruszenia ochrony danych osobowych, a następnie niezwłocznie przekazuje jego kopię administratorowi danych.

6) Raport o którym mowa w ppkt. 5 lit. c) zawiera w szczególności:

a. opis okoliczności naruszenia ochrony danych osobowych;

b. opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazuje kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;

c. opis możliwych konsekwencji naruszenia ochrony danych osobowych;

d. ocenę czy jest prawdopodobne, że naruszenie skutkowało ryzykiem lub wysokim ryzykiem naruszenia wolności lub praw osób fizycznych;

e. wskazanie zastosowanych lub proponowanych działań zaradczych, ze szczególnym uwzględnieniem takich, które zmierzają do zminimalizowania ewentualnych negatywnych skutków naruszenia.

7) Administrator danych osobowych po zapoznaniu się z raportem o którym mowa w ppkt. 6) podejmuje decyzje o dalszym trybie postępowania, a w szczególności:

a. jeśli to właściwe, zarządza podjęcie czynności zmierzających do usunięcia naruszenia i jego skutków oraz zapobieżeniu naruszeniom ochrony danych osobowych na przyszłość.

b. jeśli to możliwe, zarządza zastosowanie środków eliminujących lub zmniejszających prawdopodobieństwo ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,

c. jeśli jest to właściwe zawiadamia o naruszeniu właściwe organy, w tym zgłasza naruszenie organowi nadzorczemu oraz informuje o naruszeniu osoby, których naruszenie dotyczy. Do zgłasza naruszeni organowi nadzorczemu zgodnie z art. 33 ust. 1 RODO oraz zawiadamia o naruszeniu osób, których dane dotyczą zgodnie z art. 34 ust. 1 RODO stosuje się postanowienia pkt. 2 i 3 niniejszej części.

2. Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu.

1) Jeśli administrator danych ustali, że jest prawdopodobne, że naruszenie ochrony danych osobowych stwierdzone w trybie określonym w pkt. 1 skutkowało ryzykiem naruszenia wolności lub praw osób fizycznych nakazuje koordynatorowi procesów biznesowych przygotowanie projektu zgłoszenia naruszenia organowi nadzorczemu,

2) Zgłoszenie naruszenia wskazane w ppkt. 1) zawiera, w szczególności:

a. informacje zawarte w raporcie, zgodnie z pkt. 1 ppkt. 6),

b. wskazanie imienia i nazwiska oraz danych kontaktowych inspektora ochrony danych osobowych jako osoby właściwej do kontaktu w sprawie. W szczególnych przypadkach, po konsultacji z administratorem danych osobowych, do kontaktu w sprawie może być wskazana inna osoba niż inspektor ochrony danych osobowych.

3) Zgłoszenie naruszenia ochrony danych osobowych, o którym mowa w ppkt. 1-2) administrator danych zatwierdza i przekazuje organowi nadzorczemu bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia.

4) Jeżeli dotrzymanie terminu wskazanego w ppkt. 3) jest niemożliwe administrator danych do zgłoszenia dołącza wyjaśnienie przyczyn opóźnienia. Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić od razu, administrator danych udziela tych informacji sukcesywnie, bez zbędnej zwłoki.

3. Zawiadomienie osoby, której dane dotyczą.

1) Jeśli administrator danych ustali, że naruszenie ochrony danych osobowych stwierdzone w trybie określonym w pkt. 1 może powodować wysokie ryzyko naruszenia wolności lub praw osób fizycznych i nie da się zastosować środków eliminujących to wysokie ryzyko, nakazuje koordynatorowi procesów biznesowych przygotowanie projektu zawiadomienia o naruszeniu dla wszystkich osób, których danych naruszenie dotyczy.

2) Zawiadomienie o którym mowa w ppkt. 1) powinno być napisane jasnym i prostym językiem oraz zawierać, w szczególności:

a. opis charakteru naruszenia,

b. opis możliwych konsekwencji naruszenia,

c. wskazanie zastosowanych lub planowanych działań zaradczych, ze szczególnym uwzględnieniem takich, które

mogą zminimalizować ewentualne negatywne skutki naruszenia,

d. wskazanie imienia i nazwiska oraz danych kontaktowych koordynatorowi procesów biznesowych, jako osoby właściwej do kontaktu w sprawie. W szczególnych przypadkach, po konsultacji z administratorem danych osobowych, do kontaktu w sprawie może być wskazana inna osoba niż koordynator procesów biznesowych.

3) Zawiadomienie o naruszeniu ochrony danych osobowych administrator danych zatwierdza i przekazuje niezwłocznie wszystkim osobom, których danych naruszenie dotyczy.

4) Jeżeli administrator danych oceni, że realizacja wymogów określonych w ppkt. 1-3) wymagałoby niewspółmiernie dużego wysiłku, w szczególności niewspółmiernie dużego wysiłku wymagałoby nawiązanie bezpośredniego, indywidualnego kontaktu z osobami, których danych naruszenie dotyczy, może podjąć decyzje o przekazaniu informacji zainteresowanym poprzez wydanie publicznego komunikatu lub o zastosowaniu innego podobnego środka, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

4. Dokumentacja naruszenia ochrony danych osobowych.

1) Inspektor ochrony danych osobowych prowadzi dokumentację naruszenia danych osobowych.
2) W skład dokumentacji o której mowa w ppkt. 1) wchodzą:

a. kopia raportu o którym mowa w pkt. 1 ppkt. 6,
b. kopia zgłoszenia o którym mowa w pkt. 2
c. kopie zawiadomień o których mowa w pkt. 3
d. wszelkie inne dokumenty, w tym notatki służbowe, pliki, zdjęcia i inne dowody zebrane w trakcie przeprowadzania czynności wyjaśniających pozwalające ustalić okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.

3) Dokumentacja naruszenia ochrony danych osobowych pozostaje do wglądu organu nadzorczego.

IX. PRZEPISY PRZEJŚCIOWE

1) Niniejsza *Polityka ochrony danych osobowych* w IT CONNECT Sp. z o.o, została zaktualizowana w dniu 04.12.2019 roku, a obowiązuje od 01.05.2018.
2) Niniejsza *Polityka ochrony danych osobowych* w IT CONNECT Sp. z o.o weszła w życie dnia 01.05.2018. Do 25 maja 2018 r. należy ją jednak traktować jako *Politykę bezpieczeństwa informacji* w rozumieniu §3 ust. 1 i §4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r., w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100 poz. 1024).
3) W razie wątpliwości wszyscy przetwarzający dane osobowe w IT CONNECT Sp. z o.o, zobowiązani są do 25 maja 2018 r. tak interpretować postanowienia niniejszej *Polityki,* aby postępować zgodnie z aktualnie obowiązującymi przepisami o ochronie danych osobowych, a w szczególności z postanowieniami: ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. DzU z 2016, poz. 922 z późn. zm.), rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (DzU nr 100, poz. 1024) oraz rozporządzenia Ministra Administracji I Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (DzU, poz. 745).
4) Wszyscy przetwarzający dane osobowe w IT CONNECT Sp. z o.o, zobowiązani są dostosować swoje działania do wymogów niniejszej *Polityki*.

X. POSTANOWIENIA KOŃCOWE

1) Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się i stosować

do zasad i procedur określonych w niniejszej *Polityce*.

2) Naruszenie zasad i procedur określonych w niniejszej *Polityce* może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 Kodeksu pracy.
3) Naruszenie zasad i procedur określonych w niniejszej *Polityce* może być potraktowane jako nienależyte wykonanie umowy w rozumieniu Kodeksu cywilnego.

Decyzja do *Polityki ochrony danych osobowych* nr 1

Decyzja w sprawie mianowania administratora systemu

W dniu 30.04.2018 decyzją Prezesa Zarządu Grzegorza Skoczka został mianowany na stanowisko Administratora Systemu w firmie IT CONNECT Sp. z o.o. Pan Bartłomiej Mańkowski, który od dnia 01.05.2018 realizuje wszelkie wynikające z tego tytułu zadania i obowiązki wskazane w wewnętrznym dokumencie Polityka ochrony danych osobowych oraz Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych .

……..

Podpis

Decyzja do *Polityki ochrony danych osobowych* nr 2

Decyzja w sprawie mianowania koordynatora procesów biznesowych przez Prezesa Zarządu Grzegorza Skoczka

W dniu 30.04.2018 decyzją Prezesa Zarządu Grzegorza Skoczka została mianowana na stanowisko Koordynatora Procesów Biznesowych w firmie IT CONNECT Sp. z o.o. Pani Aleksandra Kasta-Pyz, która od dnia 01.05.2018 realizuje wszelkie wynikające z tego tytułu zadania i obowiązki wskazane w wewnętrznym dokumencie Polityka ochrony danych osobowych.

……..

Podpis

Adnotacja z dnia 14.02.2019

W dniu 14.02.2019 na stanowisko został powołany Inspektor Ochrony Danych Osobowych (Akt powołania Inspektora dołączony do *Polityki*) .
Wszystkie obowiązki Koordynatora Procesów Biznesowych zostały przekazane Inspektorowi.

Dodatek do *Polityki ochrony danych osobowych nr 1*

Procedura przydzielania identyfikatora i hasła w firmie IT CONNECT Sp. z o.o..*

Inspektor danych osobowych składa wniosek drogą elektroniczną o przydzielenie użytkownikowi identyfikatora i hasła, podając administratorowi systemu imię i nazwisko użytkownika.

Administrator systemu po przydzieleniu ww. danych użytkownikowi przekazuję taką informację bezpośrednio użytkownikowi w trakcie spotkania.

*Szczegółowe informacje na temat ww. procedury zawiera *Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w IT CONNECT Sp.*

Dodatek do *Polityki ochrony danych osobowych nr 1*

Procedura nadawania upoważnień do przetwarzania danych osobowych w firmie IT CONNECT Sp. z o.o.*

Inspektor ochrony danych osobowych występuje drogą elektroniczną z wnioskiem do administratora danych o nadanie upoważnienia w określonym zakresie do przetwarzania danych osobowych dla wskazanej osoby (podanie imienia i nazwiska osoby, oraz numeru PESEL)

Administrator danych drogą mailową informuje inspektora ochrony danych osobowych o zgodzie na upoważnienie lub braku zgody.

*Szczegółowe informacje na temat ww. procedury zawiera *Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w IT CONNECT Sp.*