Spis treści

I. PRZEDMIOT / CEL

Niniejsza Polityka Ochrony Danych Osobowych Jastim powstała w oparciu o analizę charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia. Jej podstawowym celem jest uregulowanie wszystkich obszarów, które odnoszą się do procesów przetwarzania danych oraz przyjętych w Jastim środków technicznych i organizacyjnych.

II. ODPOWIEDZIALNOŚĆ

a. Nadzór nad aktualnością niniejszego dokumentu sprawuje Zarząd Jastim oraz IOD.
b. Każdorazowa zmiana bądź aktualizacja niniejszej polityki wymaga konsultacji z powołanym w Jastim inspektorem ochrony danych (IOD).

III. ZAWARTOŚĆ

Rozdział 1. Słowniczek

§ 1.

Przez użyte w Polityce Ochrony Danych Osobowych (PODO) terminy należy rozumieć:

1) **administrator danych** – Jastim Sp. z o.o., czyli osoba prawna która samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;
2) **audyt** – systematyczny, niezależny i udokumentowany proces uzyskiwania dowodu z audytu oraz jego obiektywnej oceny w celu określenia stopnia spełnienia kryteriów audytu;
3) **dane osobowe** - oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

4) **dostępność** – właściwość określającą, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie, w założonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym;
5) **incydent bezpieczeństwa** – każde wykryte naruszenie albo wykryta próba naruszenia bezpieczeństwa danych osobowych będąca naruszeniem obowiązujących przepisów wewnętrznych Jastim lub powszechnie obowiązujących przepisów prawa; źródłem incydentu bezpieczeństwa może być zarówno przypadkowe, jak i celowe działanie albo jego zaniechanie przez pracowników / współpracowników lub osoby, przy pomocy których Jastim wykonuje swoje czynności;
6) **inspektor ochrony danych (IOD)** – osoba wyznaczona do realizacji zadań wskazanych w art. 39 RODO;
7) **integralność** – właściwość polegającą na tym, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony;
8) **naruszenie ochrony danych osobowych** - oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
9) **ocena ryzyka** – proces mający na celu oszacowanie wagi ryzyka rozumianej jako funkcja prawdopodobieństwa wystąpienia skutku i krytyczności jego następstw dla praw lub wolności osób fizycznych, których dane osobowe przetwarza Jastim ;
10) **organ nadzorczy** – Prezes Urzędu Ochrony Danych Osobowych (PUODO);
11) **podatność systemu teleinformatycznego** - właściwość systemu teleinformatycznego, która może być wykorzystana przez co najmniej jedno zagrożenie;
12) **podmiot przetwarzający (procesor)** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
13) **polityka ochrony danych osobowych (PODO)** – niniejszy dokument, przez który należy rozumieć zestaw efektywnych, udokumentowanych zasad i procedur bezpieczeństwa wraz z ich planem wdrożenia i egzekwowania;
14) **postępowanie z ryzykiem** - proces modyfikowania ryzyka; postępowanie z ryzykiem może uwzględniać np. unikanie ryzyka poprzez decyzję o nierozpoczynaniu lub niekontynuowaniu działań powodujących ryzyko, usunięcie źródła ryzyka, zachowanie ryzyka na podstawie świadomej decyzji;

15) **poufność** – właściwość zapewniająca, że dane osobowe nie są udostępniane lub wyjawiane nieupoważnionym osobom fizycznym;
16) **pracownicy i współpracownicy IT** – osoby nadzorujące pracę systemu teleinformatycznego oraz wykonujące czynności wymagające specjalnych uprawnień lub osoby nadzorujące wykonywanie tych czynności przez pomiot (podmioty) zewnętrzny na podstawie umowy (umów) zawartej z Jastim;
17) **proces przetwarzania danych** – seria powiązanych ze sobą działań lub zadań, które rozwiązują określony problem lub prowadzą do osiągnięcia określonego efektu przy wykorzystaniu danych osobowych;
18) **profilowanie** - oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
19) **przetwarzanie** - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
20) **RODO** - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE;
21) **rozliczalność** – właściwość zasobu informatycznego oznaczająca, że wykonane na nim działania mogą być jednoznacznie przypisane wykonującej je osobie lub systemowi informatycznemu;
22) **ryzyko** – prawdopodobieństwo tego, że zagrożenie wykorzysta podatność powodując skutek;
23) **system teleinformatyczny** - zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i

odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego w rozumieniu ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne;

24) **system ochrony danych osobowych (SODO)** – polityka ochrony danych osobowych, procedury, wytyczne, związane zasoby i działania, wspólnie zarządzane przez Jastim dążące do ochrony danych osobowych, które przetwarza;
25) **użytkownik** – pracownik lub współpracownik Jastim oraz inne osoby, przy pomocy których Jastim wykonuje swoje czynności, posiadające uprawnienia do pracy w systemie teleinformatycznym zgodnie z zakresem obowiązków służbowych i nadanymi uprawnieniami;
26) **właściciel biznesowy** - osoba odpowiedzialna za działanie i ciągłe ulepszanie danego procesu przetwarzania danych;
27) **zagrożenie** – stan faktyczny, który może spowodować naruszenie bezpieczeństwa danych osobowych;
28) **zagrożenie systemu teleinformatycznego** - potencjalna przyczyna niepożądanego zdarzenia, która może wywołać szkodę w systemie teleinformatycznym;
29) **zasada wiedzy koniecznej** – dostęp pracowników i współpracowników Jastim lub osób, przy pomocy których Jastim wykonuje swoje czynności na danych osobowych, ograniczony wyłącznie do tych danych, które są im niezbędne do wykonania powierzonych zadań.

Rozdział 2. Podstawy prawne

§ 2.

Niniejsza Polityka Ochrony Danych Osobowych opiera się na:

1) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (w dalszej części jako RODO);
2) Ustawie z dnia 10 maja 2018 o ochronie danych osobowych (UODO);
3) Ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (w dalszej części jako UŚUDE);

4) Ustawie z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (w dalszej części jako PT);
5) PN-ISO/IEC 27001:2013;
6) PN-ISO/IEC 27005:2014;
7) Wytycznych Grupy Roboczej Art. 29 Ds. Ochrony Danych Osobowych tj.:
    a) Wytyczne dotyczące inspektorów ochrony danych ('DPO') z dnia 13 grudnia 2016 r.;
    b) Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) oraz ustalenia, czy przetwarzanie „z dużym prawdopodobieństwem może powodować wysokie ryzyko" do celów rozporządzenia 2016/679 z dnia 4 kwietnia 2017 r.;
    c) Wytyczne dotyczące prawa do przenoszenia danych z dnia 13 grudnia 2016 r.;
    d) Wytyczne dotyczące ustalenia wiodącego organu nadzorczego właściwego dla administratora lub podmiotu przetwarzającego z dnia 13 grudnia 2016 r.

Rozdział 3. Deklaracja stosowania

§ 3.

1) Zarząd Jastim, świadomy odpowiedzialności za zapewnienie bezpieczeństwa danych osobowych, deklaruje gotowość budowy kompleksowego systemu ochrony danych osobowych (SODO) oraz wsparcie wszelkich działań mających na celu ochronę danych osobowych przetwarzanych przez Jastim.
2) Zarząd Jastim, z uwagi na to, że istotnym elementem działalności biznesowej Jastim jest przetwarzanie danych osobowych, podjął decyzję o powołaniu inspektora ochrony danych (IOD). Szczegółowy zakres zadań i statut IOD zostały określone w procedurze „Zadania i status Inspektora Ochrony Danych" stanowiącej **załącznik nr 1** do PODO.
3) Zarząd Jastim zobowiązuje dział IT do:
    a) informowania Zarządu Jastim o potrzebach w zakresie niezbędnych środków technicznych, które zapewniać będą bezpieczeństwo danych osobowych;
    b) wdrożenia niezbędnych środków technicznych i organizacyjnych mających na celu zabezpieczenie infrastruktury IT oraz systemów teleinformatycznych służących do przetwarzania danych osobowych;
    c) dbania o zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów teleinformatycznych i usług przetwarzania;

d) dbania o zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego mającego związek z systemami teleinformatycznymi i infrastrukturą IT służącymi do przetwarzania danych osobowych;
e) regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych w ramach systemów teleinformatycznych i infrastruktury IT.

4) W celu uszczegółowienia zasad wskazanych w PODO Zarząd Jastim może wyznaczyć osobę bądź osoby odpowiedzialne za opracowanie dokumentacji ochrony danych osobowych obejmującej szczegółowe polityki, instrukcje i procedury wynikające z PODO oraz do wdrożenia i utrzymania właściwego poziomu bezpieczeństwa danych osobowych wynikającego z tych uregulowań.

Rozdział 4. Cel i zakres PODO

§ 4.

1) Celem PODO jest stworzenie podstaw organizacyjnych dla wdrożenia RODO w Jastim.
2) PODO odnosi się do wszelkich danych osobowych znajdujących się w posiadaniu Jastim niezależnie od tego w jaki sposób te dane są przetwarzane.
3) Zasady ustanowione w PODO powinny być stosowane przez wszystkie osoby zatrudnione w Jastim/ współpracujące z Jastim.

Rozdział 5. Czynniki zewnętrzne i wewnętrzne istotne dla celu działania Jastim

§ 5.

1) Czynniki zewnętrzne mające wpływ na działalność Jastim (kontekst zewnętrzny) w zakresie dotyczącym bezpieczeństwa danych osobowych:
   a) powszechnie obowiązujące przepisy prawa w zakresie ochrony danych osobowych;
   b) pozycja rynkowa Jastim;
   c) współpraca z innymi podmiotami i partnerami biznesowymi;
   d) oczekiwania klientów, kontrahentów.

2) Czynniki wewnętrzne mające wpływ na działalność Jastim (kontekst wewnętrzny) w zakresie dotyczącym bezpieczeństwa danych osobowych:
   a) wewnętrzne regulacje i procedury obowiązujące w Jastim;
   b) struktura organizacyjna Jastim;
   c) zobowiązania i uprawnienia Jastim wynikające z zawartych umów i porozumień;
   d) cele opisane w niniejszej PODO.

Rozdział 6. Role i odpowiedzialność za bezpieczeństwo danych osobowych

§ 6.

Szczególna rola i odpowiedzialność za bezpieczeństwo danych osobowych spoczywa na:

a) Zarządzie Jastim;
b) Dyrektorach/Managerach poszczególnych działów;
c) Dziale IT;
d) Inspektorze Ochrony Danych (IOD).

§ 7.

1) Zarząd Jastim sprawuje nadzór nad bezpieczeństwem danych osobowych, w szczególności odpowiada za odpowiednią strukturę organizacyjną i podział zadań zapewniający bezpieczeństwo danych i systemów teleinformatycznych.
2) Do zadań Zarządu Jastim należy:
   a) prawna odpowiedzialność za funkcjonowanie Jastim, w tym również za przestrzeganie wymagań związanych z zabezpieczeniem danych osobowych i systemów teleinformatycznych;
   b) zatwierdzanie i publikowanie dokumentów i procedur związanych z ochroną danych osobowych dotyczących wszystkich pracowników i współpracowników Jastim;
   c) zapewnienie wsparcia organizacyjno-finansowego przy wdrażaniu mechanizmów zabezpieczenia danych osobowych i systemów teleinformatycznych;
   d) zapewnienie odpowiednich pomieszczeń (stosownie zabezpieczonych i wyposażonych) do procesu przetwarzania i przechowywania danych osobowych;
   e) uwzględnianie kryterium wiarygodności zatrudnianych pracowników i współpracowników przy rekrutacji na stanowiska związane z dostępem do

krytycznych danych osobowych lub z administracją krytycznych komponentów systemów teleinformatycznych;

f) zaznajomienie pracowników i współpracowników z prawnymi oraz pracowniczymi konsekwencjami naruszenia bezpieczeństwa danych osobowych (za pośrednictwem IOD);
g) zapewnienie pracownikom i współpracownikom szkoleń w zakresie poszerzania wiedzy i świadomości związanej z bezpieczeństwem danych osobowych oraz stosowanymi rozwiązaniami używanymi w celu utrzymania bądź zapewnienia odpowiedniego poziomu zabezpieczeń stosowanych w procesach przetwarzania i gromadzenia danych (co do zasady szkolenia w powyższym zakresie prowadzi IOD);
h) wyznaczenie i powołanie IOD.

§ 8.

Do zadań dyrektorów/managerów, w tym w szczególności właścicieli biznesowych dla poszczególnych procesów przetwarzania danych, należy:

a) nadzór nad przestrzeganiem zasad i procedur składających się na PODO w pracy kierowanego działu;
b) promowanie i wymaganie postaw zgodnych z zasadami bezpieczeństwa danych osobowych przyjętymi w Jastim, w tym reakcja na wszelkie wykryte nieprawidłowości;
c) przekazywanie, bezpośrednio po wykryciu naruszenia ochrony danych osobowych, stosownej informacji o takim naruszeniu do ……, Zarządu oraz IOD (uwaga – w przypadkach szczególnych Jastim ma obowiązek zgłosić naruszenie do Prezesa Urzędu Ochrony Danych Osobowych i ma na to 72 godziny liczone od wykrycia naruszenia, stąd reakcja dyrektora/managera musi być niezwłoczna); informacja taka powinna zawierać:
   - opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
   - opis możliwych konsekwencji naruszenia ochrony danych osobowych, na tyle na ile jest to możliwe;

d) identyfikowanie podatności i zagrożeń dla nadzorowanych procesów przetwarzania danych i przekazywanie w tym zakresie informacji do Działu IT oraz IOD;
e) uczestniczenie w procesie oceny i postępowania z ryzykiem, które odnosi się do nadzorowanych przez danego dyrektora (lub innego właściciela procesu) procesów przetwarzania danych;
f) współpraca z innymi podmiotami i osobami odpowiedzialnymi za bezpieczeństwo danych osobowych w Jastim.

§ 9.

Do zadań Działu IT oraz pracowników i współpracowników Działu IT, oprócz tych, które zostały wprost wskazane w PODO albo jej załącznikach, należą:

a) dbanie o poprawne i efektywne działanie administrowanych systemów teleinformatycznych;
b) opiniowanie zgłoszeń w zakresie potrzeb dotyczących rozwoju systemów teleinformatycznych;
c) uczestniczenie w identyfikacji i ocenie ryzyka związanego ze środowiskiem teleinformatycznym;
d) uczestniczenie w procesie oceny i postępowania z ryzykiem;
e) wdrażanie odpowiednich środków organizacyjnych i technicznych odpowiadających zidentyfikowanym w trakcie oceny ryzyka zagrożeniom;
f) świadczenie wsparcie technicznego dla użytkowników systemów teleinformatycznych;
g) wykonywanie i/lub nadzorowanie procedury backupu danych osobowych (sporządzania kopii awaryjnych);
h) reagowanie i podejmowanie stosownych działań w odniesieniu do wykrytych incydentów naruszenia ochrony danych osobowych;
i) na wniosek …….. nadają użytkownikom prawa dostępu do systemów teleinformatycznych;
j) uczestniczenie w przygotowaniu propozycji zakresu testów, dokonywanie instalacji i uczestniczenie w testowaniu nowych wersji oprogramowania w środowisku testowym;
k) sporządzanie zapotrzebowania na oprogramowanie, sprzęt i usługi związane z technicznymi aspektami ochrony systemu teleinformatycznego;

l) dokonywanie i/lub nadzorowanie bezpiecznej eliminacji wycofanych z użytku systemów i komponentów infrastruktury teleinformatycznej;
m) odpowiedzialność za ciągłość działania systemów i infrastruktury teleinformatycznej oraz łączy teleinformatycznych;
n) dbanie o właściwe wyposażenie lokalizacji zapasowych (o ile występują), a także odpowiednie zabezpieczenie zasobów awaryjnych;
o) monitorowanie dostępności systemów teleinformatycznych;
p) odpowiedzialność za odtworzenie danych osobowych z kopii awaryjnych;
q) sprawowanie nadzoru nad działaniem zewnętrznych dostawców usług w zakresie jakości i przestrzegania standardów bezpieczeństwa danych osobowych w zakresie czynności technicznych realizowanych w związku z wykonaniem umów.

§ 10.

Szczegółowe zadania i status IOD zostały określone w dokumencie "Zadania i status Inspektora Ochrony Danych" stanowiącym **załącznik nr 1** do PODO. Szczegółowy opis kompetencji określonych osób w systemie ochrony danych osobowych został określony w dokumencie "Schemat osób funkcyjnych w systemie ochrony danych osobowych" stanowiącym **załącznik nr 2** do PODO.

§ 11.

Do zadań użytkowników, oprócz tych, które zostały wprost wskazane w PODO albo jej załącznikach, należą:

a) przestrzeganie zasad określonych w PODO i wskazanych w niej załącznikach;
b) zapewnienie poufności w stosunku do wszystkich danych osobowych przetwarzanych w Jastim;
c) zabronione jest rozpowszechnianie danych osobowych podlegających ochronie;
d) obowiązek zachowania poufności danych osobowych w Jastim w zakresie związanym z wykonywaniem przez pracowników i współpracowników zadań dla Jastim/ nie wygasa po ustaniu stosunku pracy/współpracy.

Rozdział 7. Zasady korzystania z przydzielonego sprzętu służbowego i elektronicznych nośników informacji oraz regulamin pracy zdalnej

§ 12.

Szczegółowe zasady korzystania z systemów informatycznych oraz z przydzielonego sprzętu służbowego, elektronicznych nośników informacji oraz regulamin pracy zdalnej stanowi **załącznik nr 3** do PODO.

Rozdział 8. Kontrola dostępu

§ 13.

Szczegółowa polityka kontroli dostępu do urządzeń, baz danych, oraz systemów została opisana w poniżej wskazanych dokumentach:

1) Procedura nadawania/zmiany/odbierania uprawnień dla użytkownika w systemie informatycznym stanowi **załącznik nr 4** do PODO;
2) Procedura zmiany haseł w systemach informatycznych oraz zarządzania danymi wykorzystywanymi do uwierzytelnienia stanowi **załącznik nr 5** do PODO.

Rozdział 9. Korzystanie z systemów informatycznych, poczty elektronicznej oraz tworzenie kopii zapasowych

§ 14.

Szczegółowe procedury dotyczące korzystania z systemów informatycznych, poczty elektronicznej oraz tworzenia kopii zapasowych:

1) Zasady zabezpieczenia danych osobowych na stanowisku pracy stanowią **załącznik nr 6** do PUODO.
2) Zasady pracy z pocztą elektroniczną stanowią **załącznik nr 7** do PODO;

Rozdział 10. Relacje z dostawcami, którzy uzyskują dostęp do danych osobowych Jastim

§ 15.

Szczegółowa procedura ochrony danych osobowych w relacjach z dostawcami Jastim stanowi **załącznik nr 8** do PODO.

Rozdział 11. Sposób postępowania przy naruszeniu ochrony danych osobowych

§ 16.

Szczegółowa procedura dotycząca zgłaszania naruszeń / zarządzania zdarzeniami związanymi z bezpieczeństwem danych osobowych (zasady dotyczące zgłaszania incydentów) stanowi **załącznik nr 9** do PODO.

Rozdział 12. Prawa podmiotów danych osobowych

§ 17.

Szczegółowa procedura obsługi wniosków podmiotów danych stanowi **załącznik nr 10** do PODO.

Rozdział 13. Nadawanie upoważnień do przetwarzania danych

§ 18.

Szczegółowa procedura dotycząca nadawania upoważnień do przetwarzania danych osobowych stanowi **załącznik nr 11** do PODO.

Rozdział 14. Projektowanie nowych procesów

§ 19.

Szczegółowa procedura dotycząca projektowania nowych procesów stanowi **załącznik nr 12** do PODO.

Rozdział 15. Retencja danych

§ 20.

Wytyczne dotyczące wewnętrznych okresów przechowywania danych stanowią **załącznik nr 13** do PODO.

Rozdział 16. Szkolenia i edukacja

§ 21.

1) Pracownicy i współpracownicy Jastim w zakresie odpowiednim do swoich zadań i obowiązków są zobowiązani znać treść niniejszej PODO oraz wskazanych w niej załączników.
2) Pracownicy i współpracownicy Jastim powinni zostać poinformowani o zakresie odpowiedzialności i obowiązków wynikających z niniejszej PODO wraz z konsekwencjami prawnymi i dyscyplinarnymi w przypadku jej naruszenia.
3) Wszyscy pracownicy i współpracownicy Jastim zobligowani są do uczestnictwa w szkoleniach dotyczących ochrony danych osobowych.

§ 22.

1) Szkolenia w zakresie ochrony danych osobowych przeprowadza się wstępnie przed udzieleniem upoważnienia do przetwarzania danych osobowych, cyklicznie, lub w razie potrzeby, na wniosek.
2) Szczegółowe zasady dotyczące szkoleń określone zostały w **załączniku nr 14** do PUODO (Procedura szkoleń pracowników/współpracowników Jastim).

Rozdział 17. Audyt

§ 23.

1) PODO oraz procesy zachodzące w Jastim jak również stosowana dokumentacja powinna być poddawana regularnym audytom.
2) Do przeprowadzania audytu upoważnieni są, każdy we właściwym zakresie (odpowiadającym realizowanym zadaniom służbowym):
   a) osoby zatrudnione na stanowisku audytora wewnętrznego;
   b) IOD;
   c) podmioty zewnętrzne za zgodą Zarządu Jastim.
3) Szczegółowy zakres audytu ustalany jest przez IOD i Zarząd.

4) Przeprowadzenie audytu wymaga sporządzenia jego planu, w którym określa się m.in. cel, kryteria, zakres podmiotowy i przedmiotowy.
5) Audyt zachodzących w Jastim procesów oraz stosowanej dokumentacji powinien odbyć się przynajmniej raz w roku i uwzględniać poniższe stałe elementy:
    a) przegląd wszystkich lub poszczególnych procesów;
    b) analizę stosowanej w organizacji dokumentacji w odniesieniu do wszystkich lub poszczególnych procesów;
    c) analizę kluczowych dokumentów, do prowadzenia których zobowiązany jest Jastim (rejestr upoważnień, rejestr podmiotów przetwarzających, rejestr czynności przetwarzania, rejestr kategorii czynności przetwarzania, rejestr naruszeń).
6) Wyniki audytu przedstawia się Inspektorowi Ochrony Danych (jeśli nie przeprowadzał tego audytu) oraz Zarządowi Jastim .
7) Jeżeli przeprowadzony przez IOD audyt wykaże określone niezgodności w odniesieniu do poszczególnych procesów zachodzących w Jastim czy stosowanej dokumentacji, komórką odpowiedzialną za usunięcie wskazanych niezgodności jest Zarząd.
8) IOD współpracuje z Zarządem przy usuwaniu, ujawnionych w trakcie audytu, niezgodności, o których mowa w pkt. 7 powyżej.

Rozdział 18. Przegląd i aktualizacja PODO

§ 24.

1) Przegląd PODO powinien być dokonywany co najmniej raz do roku z zastrzeżeniem postanowień ust. 2.
2) W przypadku wystąpienia znaczących zmian powinien być przeprowadzany przegląd doraźny, którego celem będzie weryfikacja zasad i ewentualne dostosowanie PODO do zmian środowiska organizacyjnego, warunków biznesowych, środowiska technicznego, a także w zakresie zachowania zgodności z przepisami powszechnie obowiązującego prawa.
3) Za aktualizację PODO odpowiedzialność ponosi wyznaczony w Jastim IOD.
4) Wszelkie zmiany w niniejszej Polityce wymagają akceptacji IOD.

IV. Załączniki

Integralną częścią niniejszej polityki są następujące załączniki:

1) Zadania i status Inspektora Ochrony Danych;
2) Schemat osób funkcyjnych w systemie ochrony danych osobowych;
3) Zasady korzystania z systemów informatycznych oraz z przydzielonego sprzętu służbowego, elektronicznych nośników informacji oraz regulamin pracy zdalnej;
4) Procedura nadawania/zmiany/odbierania uprawnień dla użytkownika w systemie informatycznym;
5) Procedura zmiany haseł w systemach informatycznych oraz zarządzania danymi wykorzystywanymi do uwierzytelnienia;
6) Zasady zabezpieczenia danych osobowych na stanowisku pracy;
7) Zasady pracy z pocztą elektroniczną;
8) Procedura ochrony danych osobowych w relacjach z dostawcami;
9) Zasady dotyczące zgłaszania incydentów;
10) Procedura obsługi wniosków podmiotów danych;
11) Procedura nadawania upoważnień do przetwarzania danych osobowych;
12) Procedura projektowania nowych procesów (uwzględniające zasady privacy by default, privacy by design);
13) Wytyczne dotyczące wewnętrznych okresów przechowywania danych;
14) Procedura szkoleń pracowników i współpracowników Jastim

	Imię i Nazwisko	**Data**	**Podpis**
Sporządził/a			
Aktualizował/a			
Zatwierdził/a			