AKTUALIZACJA POLITYKI BEZPIECZEŃSTWA

WPROWADZENIE

Pszczyńskie Towarzystwo Budownictwa Społecznego Sp. z o.o zwany dalej PTBS jako Administrator Danych Osobowych w sposób bardzo staranny stara się zapewnić bezpieczeństwo przetwarzanych przez ośrodka danych poprzez dostępne formy zabezpieczeń organizacyjnych i technicznych.

Niniejszy dokument opisuje m. in. reguły dotyczące bezpieczeństwa danych osobowych zawartych w systemach informatycznych w PTBS.

Opisane reguły określają granice dopuszczalnego zachowania wszystkich użytkowników przetwarzających dane osobowe drogą tradycyjną (papierową) oraz w systemie systemów informatycznych wspomagających pracę PTBSu. Dokument zwraca uwagę na konsekwencje jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.

Sposób postępowania z wszystkimi danymi osobowymi przetwarzanymi w Spółce zarówno w formie papierowej jak elektronicznej, odpowiednie zabezpieczenia, ochrona przetwarzanych danych, niezawodność funkcjonowania oraz okresowa kontrola stosowanych zabezpieczeń są podstawowym elementem prawidłowej polityki.

Niniejsza „**Polityka bezpieczeństwa”** jest stosowana przez wszystkie struktury organizacyjne PTBSu jak i osoby w nim zatrudnione przy przetwarzaniu tych danych a realizowana poprzez zabezpieczenia fizyczne, organizacyjne, oprogramowanie systemowe, aplikacje oraz użytkowników. Niniejszy dokument będzie również w miarę potrzeb poddawany aktualizacjom i stosownym korektom celem jak najlepszego zabezpieczenia danych osobowych znajdujących się w PTBS.

§ 1
Definicje

1. Podstawą upoważniającą Pszczyńskie Towarzystwo Budownictwa Społecznego Sp. z o.o. do przetwarzania danych osobowych są rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1) (dalej: RODO) oraz

a) ustawa o własności lokali,

b) ustawa o niektórych formach popierania budownictwa mieszkaniowego,

c) ustawa o ochronie praw lokatorów, mieszkaniowym zasobie gminy i o zmianie Kodeksu cywilnego,

d) kodeks cywilny.

2. Celem Polityki Bezpieczeństwa jest zapewnienie ochrony danych osobowych przed wszelkiego rodzaju zagrożeniami, tak wewnętrznymi jak i zewnętrznymi, świadomymi lub nieświadomymi przetwarzanych w przez Pszczyńskie Towarzystwo Budownictwa Społecznego Sp. z o.o. dla:

a) prowadzenia ewidencji i rozliczeń najemców lokali mieszkalnych,

b) prowadzenia ewidencji i rozliczeń najemców lokali użytkowych i garaży,

c) realizacji umów zarządzania nieruchomościami wspólnot mieszkaniowych,

d) rozliczania sprzedaży towarów i materiałów tj.: energia elektryczna, gaz, woda, ścieki, centralne ogrzewanie,

e) prowadzenia ewidencji wniosków o zawarcie umowy partycypacji w kosztach budowy lokalu mieszkalnego,

f) prowadzenia zadań odnoszących się do zatrudnienia pracowników i innych osób.

3. Dane osobowe w Spółce są:

a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”);

b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami („ograniczenie celu”);

c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”);

d) 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 („prawidłowość”);

e) 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 („ograniczenie przechowywania”);

f) 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 („integralność i poufność”).

Miarą bezpieczeństwa jest wielkość ryzyka związanego z ochroną danych osobowych a zarządzaniem ryzykiem które określa proces identyfikacji, kontrolowania oraz ograniczenia lub całkowitej eliminacji ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych

3. W Polityce bezpieczeństwa zostały określone definicje, które mają również zastosowanie do załączników do niniejszego dokumentu:

a) **PTBS** – rozumie się przez to Pszczyńskie Przedsiębiorstwo Budownictwa Społecznego Sp. z o.o.

b) **Dane osobowe-** to wszelkie informacje związane ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną. Osoba jest uznawana za osobę bezpośrednio lub pośrednio identyfikowalną poprzez odniesienie do identyfikatora (takiego jak nazwa, numer identyfikacyjny, dane dotyczące lokalizacji, identyfikator internetowy) albo jednego lub więcej czynników specyficznych dla danej osoby (jak np. cech fizycznych, fizjologicznych, genetycznych, umysłowych, ekonomicznych, kulturowych lub społecznych), pozwalających ustalić tożsamość tej osoby.

c) **Zbiorze danych** – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie

d) **Przetwarzaniu danych** – 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,

e) **Systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,

f) **Zabezpieczeniu danych w systemie informatycznym** - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,

g) **Usuwaniu danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,

h) **Administratorze Danych Osobowych /ADO/** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych, rozumie się przez to Zarząd PTBS

i) **Inspektor ochrony danych-** osoba wyznaczona przez administratora danych osobowych, nadzorującą przestrzeganie zasad ochrony danych osobowych, w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem

j) **Osobie upoważnionej** – osoba posiadająca upoważnienie wydane przez Administratora Danych Osobowych

k) **Użytkowniku** – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano uprawnienia do przetwarzania danych w systemie informatycznym,

l) **Identyfikatorze użytkownika (login)** – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,

m) **Haśle** – ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym

n) **Identyfikator-** ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemach informatycznych;

o) **Podmiot przetwarzający** – to osoba fizyczna lub prawna, organ publiczny, agencja lub jakkolwiek inny organ przetwarzający dane osobowe w imieniu Administratora.

p) **Pseudonimizacja danych**- oznacza przetwarzanie danych osobowych w taki sposób (np. poprzez zastępowanie nazw liczbami), że danych osobowych nie można już przypisać do określonego podmiotu danych bez użycia dodatkowych informacji (np. listy referencyjnej nazwisk i numerów), pod warunkiem, że takie dodatkowe informacje są przechowywane

oddzielnie i podlegają środkom technicznym i organizacyjnym w celu zapewnienia, że dane osobowe nie są przypisane do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,

r) **Profilowanie** – jest dowolna formą zautomatyzowanego przetwarzania danych osobowych, która 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,

s) **Anonimizacja –** zmiana danych osobowych w wyniku której dane te tracą charakter danych osobowych.

t) **Usuwanie danych**- trwałe zniszczenie danych osobowych lub ich taka modyfikacja, które nie pozwala na ustalenie tożsamości osoby, której dane dotyczą;

u) **Ograniczenie przetwarzania –** polega na oznaczeniu przetwarzanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania,

w) **Forma tradycyjna-** sposób utrwalenia danych osobowych lub innych informacji na papierze;

ż) **Zabezpieczenie danych w systemie informatycznym**- rozumie się przez to wdrożenie i eksploatację stosowanych środków technicznych i organizacyjnych, które zapewniają ochronę danych przed ich nieuprawnionym przetwarzaniem.

ź) **Osoba trzecia**- osoba spoza struktury organizacyjnej ośrodka tj. osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot którym na podstawie upoważnienia administratora lub podmiotu przetwarzającego mogą przetwarzać dane osobowe.

4. Polityka obowiązuje wszystkich obecnych i potencjalnych pracowników PTBS oraz podmiotów współpracujących na podstawie umów cywilnoprawnych, mających jakikolwiek kontakt z danymi osobowymi objętymi ochroną.

5. Przetwarzanie danych osobowych w PTBS odbywa się w wersji papierowej i elektronicznej.

6. PTBS zapewnia przestrzeganie praw osób, których dane dotyczą, w szczególności wynikających z art. 15-21 RODO.

7. PTBS nie przekazuje przetwarzanych danych osobowych do państw trzecich ani organizacji międzynarodowych w rozumieniu RODO.

8. Szczegółowy zakres obowiązków i procedur postępowania w przypadku zagrożenia bezpieczeństwa informacji określony zostanie poniżej.

§ 2
System informatyczny

Sposób zarządzania, przetwarzania oraz zabezpieczenie danych w systemie informatycznym określa Instrukcja Zarządzania Systemem Informatycznym stanowiący **załącznik nr 1** do Polityki Bezpieczeństwa.

§ 3
Inspektor Ochrony Danych

1. Administrator danych osobowych którym jest PTBS w Pszczynie celem prawidłowego nadzorowania i przestrzegania zasad ochrony danych osobowych oraz wykonywania polityki bezpieczeństwa powołała Inspektora Ochrony Danych Osobowych (IOD).
2. Zadania Inspektora Ochrony Danych Osobowych określa art. 39 Rozporządzenia Parlamentu Europejskiego (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- RODO). Do jego zadań należy:
    - organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami ww. Rozporządzenia i Ustawy o ochronie danych osobowych;
    - zapewnienie przetwarzania danych osobowych zgodnie z przyjętą Polityką bezpieczeństwa;
    - nadzorowanie wydawania i anulowania upoważnień do przetwarzania danych osobowych oraz prowadzenie stosownego rejestru upoważnień;
    - prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych;
    - prowadzenie szkoleń personelu uczestniczącego w operacjach przetwarzania danych osobowych;
    - prowadzenie okresowych audytów przetwarzania danych osobowych w placówce;
    - przeprowadzenia cyklicznej oceny ryzyka prowadzonych w PTBSie czynności przetwarzania danych osobowych oraz dokonywanie niezbędnej oceny skutków;
    - współpraca z organem nadzorczym.

§ 4
Obowiązek informacyjny

1. Celem prawidłowego obiegu informacji zarówno wewnątrz Spółki jak i osób, które korzystają z jej usług, dostosowano formę komunikacji Administrator z odbiorcami poprzez obowiązek informacyjny, która został umieszczona na stronie internetowej placówki.
2. Zgodnie z art. 13 RODO Administrator realizuje obowiązek informacyjny wobec podmiotów danych w momencie pozyskiwania od nich tych danych.
3. Wzór obowiązku informacyjnego, stanowi **załącznik nr 2** do Polityki Bezpieczeństwa.
4. Zgodnie z art. 14 RODO Administrator, jeżeli taka sytuacja będzie miała miejsce, realizuje obowiązek informacyjny również względem podmiotów danych, których dane uzyskał z innych źródeł niż bezpośrednio od podmiotu danych.

§ 5
Procedura uzyskania zgody na przetwarzanie danych osobowych

1. Administrator Danych Osobowych w przypadku pozyskania danych osobowych bezpośrednio od osoby której te dane dotyczą, powinien uzyskać jej zgodę na przetwarzanie danych osobowych oraz podać okoliczności ich przetwarzania, zgodnie z **załącznikiem nr 3** do niniejszej Polityki Bezpieczeństwa.
2. Administrator Danych Osobowych ma obowiązek poinformowania osoby, której dane dotyczą, zgodnie z **załącznikiem nr 3** o:
   - adresie swojej siedziby
   - celu zbierania danych, w szczególności o odbiorcach danych
   - prawie dostępu do treści oraz ich poprawie
   - dobrowolności lub obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.
3. Jeżeli w związku z przetwarzaniem danych osobowych w Spółce osoba, które dane dotyczą, zgłasza zamiar realizacji któregokolwiek prawa lub wolności przewidzianego w RODO, PTBS podejmuje decyzję co do uwzględnienia tego żądania, mając

na uwadze RODO i inne obowiązujące przepisy prawa. Jeżeli żądanie zostanie zgłoszone innej osobie niż PTBS, wówczas osoba ta niezwłocznie przekazuje je Spółce.

§ 6

1. Obszar przetwarzania danych osobowych stanowią pomieszczenia w siedzibie PTBS /Pszczyna, ul. Jana Kilińskiego 5a/, w których wykonywane są operacje na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie z użyciem stacjonarnego sprzętu komputerowego lub w formie kartotek, skorowidzów, ksiąg, wykazów i innych zbiorów ewidencyjnych.
2. Wykaz pomieszczeń określa **załącznik nr 4** do niniejszej Polityki Bezpieczeństwa.
3. Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób zatrudnionych, w sposób uniemożliwiający dostęp osób trzecich. Osoby postronne mogą przebywać wewnątrz wyżej wymienionego obszaru jedynie w obecności osoby upoważnionej do przetwarzania danych osobowych. W pomieszczeniach, w których przebywają osoby postronne, monitory stanowisk dostępu powinny być ustawione w sposób uniemożliwiający wgląd w dane osobom trzecim.

§ 7

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

1. Dane osobowe przetwarzane są przy wykorzystaniu systemu Miscrosoft Office oraz programu Mieszczanin /Elektroniczne Zarządzanie Nieruchomościami/ zakupionego od M.INFORMATYKA Sp. z o.o. Sp. k.
2. Identyfikację zbiorów danych osobowych przetwarzanych w PTBS wraz ze wskazaniem programów zastosowanych do ich przetwarzania zawiera **załącznik nr 5** do niniejszej Polityki Bezpieczeństwa.

§ 8

Opis struktury zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych i powiązania między nimi

1. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi zawiera **załącznik nr 6** do niniejszej Polityki Bezpieczeństwa.
2. Szczegóły opisu struktury zbiorów danych działających w ramach programu Mieszczanin opisuje:
   - instrukcja obsługi programu Centrala – Mieszczanin,
   - instrukcja obsługi programu System Łatwej Obsługi Nieruchomości – Mieszczanin,
   - instrukcja obsługi programu Techniczna Obsługa Nieruchomości – Mieszczanin.

Sposób współpracy pomiędzy różnymi systemami informatycznymi, stosowanymi w PTBS określa **załącznik nr 7** do niniejszej Polityki Bezpieczeństwa.

§ 9

Upoważnienie do przetwarzania danych osobowych

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z następującymi dokumentami:
   - Rozporządzeniem RODO,,
   - niniejszą Polityką Bezpieczeństwa oraz Instrukcją Zarządzania Systemem Informatycznym.
2. Zapoznanie się z przepisami wymienionymi w punkcie 1 pracownik potwierdza własnoręcznym podpisem na oświadczeniu, którego wzór stanowi **załącznik nr 8** do Polityki Bezpieczeństwa. Dodatkowo pracownicy podpisali zgodę na wykorzystywanie swoich danych osobowych niezbędnych do realizacji procesu zatrudnienia, w tym na przetwarzanie swojego wizerunku (zdjęć) znajdujących się na dokumentach oraz dokumentach potwierdzających poprzedni okres zatrudnienia, który stanowi załącznik nr **08 a** do niniejszej Polityki.
3. Przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu przez osobę, której powierzono obowiązki informatyka dla każdego użytkownika systemu unikalnego identyfikatora i hasła ze wskazaniem zakresu dostępnych danych i operacji.

4. Wzór formularza nadającego uprawnienia w zakresie dostępu do systemu informatycznego stanowi **załącznik nr 9** do Polityki Bezpieczeństwa.
5. Rejestr osób upoważnionych do przetwarzania danych osobowych /**załącznik nr 10** do Polityki Bezpieczeństwa/ powinien odzwierciedlać aktualny stan systemu w zakresie użytkowników i ich uprawnień oraz umożliwiać przeglądanie historii zmian uprawnień użytkowników. Administrator Danych Osobowych zobowiązany jest do prowadzenia i ochrony rejestru użytkowników.
6. Po zakończeniu stosunku pracy niezależnie od przyczyny pracownik podpisuje odwołanie upoważnienie, które stanowi **załącznik nr 11** do Polityki Bezpieczeństwa.
7. Administrator Systemu Informatycznego za wiedzą Administratora Danych Osobowych przekazuje użytkownikowi ustnie identyfikator (login) dostępowy do komputera, bądź konkretnego programu wraz z hasłem, który objęty jest tajemnicą, również po upływie jego ważności i znany jest jedynie osobie do tego upoważnionej oraz Administratorowi Systemów Informatycznych oraz Administratorowi Danych Osobowych.
8. Pracownicy zobowiązani są również do:
   a. ścisłego przestrzegania zakresu nadanego im upoważnienia;
   b. zachować w tajemnicy udostępnione dane osobowe oraz sposobów ich zabezpieczenia u Administratora;
   c. natychmiastowego zgłaszania wszelkich incydentów, zdarzeń mogących stanowić naruszenie bezpieczeństwa danych bezpośrednio do Administratora.
9. Naruszenie przyjętych w ośrodku zasad i przepisów ochrony danych osobowych może stanowić ciężkie naruszenie podstawowych obowiązków pracowniczych.
10. Za naruszenie lub próbę naruszenia zasad przetwarzania i ochrony danych osobowych zwanych dale „danymi” uważa się m.in:
    a. naruszenie bezpieczeństwa systemów informatycznych (m.in. niezmienianie lub przyjęcie hasła poniżej ustalonych u Administratora standardów, dzielenie się swoimi loginami i hasłami, logowanie się do systemów sieciowych przez niezabezpieczone sieci publiczne, otwieranie podejrzanych załączników, pozostawienie otwartych komputerów bez opieki);
    b. umożliwienie dostępu lub udostępnienie danych podmiotom do tego nieupoważnionym;
    c. zaniechanie, nawet nieumyślne, dopełnienia obowiązku ochrony przetwarzanych danych;

d. nie przestrzeganie obowiązku zachowania w tajemnicy danych oraz sposobów ich zabezpieczenia;
e. przetwarzanie danych niezgodnie z założonym zakresem i celem ich zbierania;
f. spowodowanie uszkodzenia, zgubę, niekontrolowaną zmianę lub nieuprawnione kopiowanie danych;
g. naruszenie praw osób, których dane dotyczą i są przetwarzane.

§ 10

Administrator danych osobowych celem skutecznej realizacji zapisków Polityki Bezpieczeństwa jest obowiązany do wprowadzenia odpowiednich środków technicznych, organizacyjnych oraz fizycznych.

1. Formy zabezpieczeń pomieszczeń, w których przetwarzane są dane osobowe:

a) budynek, w którym zlokalizowany jest obszar przetwarzania danych osobowych, jest wyposażony w system alarmowy oraz monitoring wizyjny zewnętrzny. Pracownicy zostali powiadomieni o monitoringu w siedzibie Administratora i wyrazili zgodę na wykorzystanie swojego wizerunku na oświadczeniu o monitoringu stanowiącego załącznik nr **08 b** do niniejszej polityki

b) wszystkie pomieszczenia, w których przetwarzane są dane osobowe zamykane są na klucz, w przypadku opuszczenia przez ostatnią osobę upoważnioną do przetwarzania danych osobowych. Po zakończeniu pracy pracownicy zamykają pokoje, po godzinach pracy wstęp do pokoju możliwy jest tylko przez osobę sprzątającą pomieszczenie lub pracownika posiadającego zezwolenie Dyrektora na pracę w godzinach poza harmonogramem lub w dniach wolnych od pracy.

c) dane osobowe przechowywane w wersji tradycyjnej (papierowej) lub elektronicznej (pamięć flash, płyty CD, /DVD, dyski) po zakończeniu pracy są przechowywane w zamykanych na klucz pokojach, a tam gdzie jest to możliwe w szafach zamykanych na klucz,

d) nieaktualne lub błędne wydruki zawierające dane osobowe niszczone są w niszczarce.

2. Formy zabezpieczeń przed nieautoryzowanym dostępem do danych osobowych:

a) podłączenie urządzenia końcowego (komputera, drukarki) do sieci komputerowej PTBS dokonywane jest na polecenie Administratora Danych Osobowych, przez osobę, której powierzono obowiązki informatyka,

b) udostępnianie użytkownikowi zasobów sieci zawierających danych osobowe przez administratora Sieci następuje na podstawie upoważnienia do przetwarzania danych osobowych,

c) identyfikacja użytkownika w systemie następuje poprzez zastosowanie uwierzytelniania,

d) przydzielenie indywidualnego identyfikatora każdemu użytkownikowi,

e) udostępnienie kluczy do pomieszczeń, w których przetwarzane są dane osobowe tylko osobom upoważnionym,

f) ustawienie monitorów na stanowiskach pracy w sposób uniemożliwiający wgląd w dane osobowe.

3. Formy zabezpieczeń przed utratą danych osobowych w wyniku awarii:

a) odrębne zasilanie sprzętu komputerowego lub zastosowanie zasilaczy zapasowych UPS lub listew antyprzepięciowych,

b) ochrona przed utratą danych poprzez cykliczne wykonywanie kopii zapasowych,

c) zastosowanie ochrony przeciwpożarowej,

d) zastosowanie firewall – systemu izolacji selekcji połączeń z siecią zewnętrzną.

4. Organizację ochrony danych osobowych realizuje się poprzez:

a) zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych przed dopuszczeniem do pracy,

b) przeszkolenie osób w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem danych i programów,

c) kontrolowanie pomieszczeń budynku,

d) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,

5. Nadzór nad przestrzeganiem zasad ochrony przetwarzanych danych osobowych sprawuje Administrator Danych Osobowych. Zadania administratora danych osobowych polegające na:

a) opracowaniu i aktualizacji „Polityki Bezpieczeństwa”;

b) prowadzeniu wykazu zbiorów danych osobowych przetwarzanych w PTBS;

c) prowadzeniu zbioru upoważnień osób upoważnionych do przetwarzania danych osobowych, zgodnie z formularzem stanowiącym **załącznik nr 10** do niniejszej Polityki Bezpieczeństwa;

d) realizowaniu procedur związanych ze zgłaszaniem Prezesowi Urzędu Ochrony Danych Osobowych zbiorów danych osobowych podlegających rejestracji oraz administratora bezpieczeństwa informacji w przypadku obowiązku jego rejestracji;

e) przeprowadzaniu szkoleń z zakresu ochrony danych osobowych dla osób upoważnionych do przetwarzania danych osobowych,

a) opracowaniu i aktualizacji instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych;
b) dokonywaniu okresowej analizy zagrożeń dla bezpieczeństwa danych osobowych oraz opracowanie w tym zakresie sprawozdania dla Administratora Danych Osobowych.
c) wdrażaniu zmian w Polityce Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym w celu zapewnienia właściwego poziomu ochrony przetwarzanych danych osobowych;
d) prowadzeniu ewidencji osób upoważnionych do przetwarzania danych osobowych.
6. Mechanizm zabezpieczania i uwierzytelniania użytkowników oraz procedury postępowania zostały szczegółowo opisane w Instrukcji Zarządzania Systemem Informatycznym, określającej sposób zarządzania systemem informatycznym w PTBS, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji.
7. Jeżeli wynika to z przepisów RODO PTBS prowadzi rejestr, w którym ujawniane są czynności przetwarzania danych osobowych dokonywane w Spółce.
8. Do zastosowanych środków organizacyjnych należą przede wszystkim następujące zasady:

- Zapoznanie każdej osoby z dokumentacją prawną dotyczącą ochrony danych osobowych, przed dopuszczeniem jej do pracy przy przetwarzaniu danych osobowych oraz zobowiązanie jej do zachowania tajemnicy służbowej,
- Prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
- Przeszkolenie osób, o których mowa w pkt. 1 § 12, w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych,
- Wyznaczenie Inspektora Danych Osobowych,
- Kontrolowanie otwierania i zamykania pomieszczeń, w których są przetwarzane dane osobowe, polegające na otwarciu pomieszczenia przez pierwszą osobę, która rozpoczyna pracę oraz zamknięciu pomieszczenia przez ostatnią wychodzącą osobę.
- Administrator wraz z powołanym Inspektorem Ochrony Danych zobowiązuje się do cyklicznego przeglądu obowiązujących w placówce zabezpieczeń.

<u>Wnioski.</u>

a) do pomieszczeń w których następuje przetwarzanie danych osobowych mają dostęp tylko uprawnione osoby bezpośrednio związane z wykonywanymi czynnościami,

b) zabezpieczenie przed nieuprawnionym dostępem do danych, nadzorowane jest przez Administratora Bezpieczeństwa zgodnie z przyjętymi procedurami nadawania uprawnień do systemu informatycznego,
c) w pomieszczeniach, w których znajdują się serwery powinna być zapewniona właściwa temperatura i wilgotność powietrza dla sprzętu komputerowego,
d) w pobliżu wejścia do pomieszczenia z serwerami i innym urządzeniami znajduje się gaśnica, która okresowo jest napełniana i kontrolowana przez specjalistę.

Wykonanie postanowień tego dokumentu ma zapewnić właściwą reakcję, ocenę i udokumentowanie przypadków naruszania bezpieczeństwa systemów oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w systemach informatycznych Pszczyńskiego Towarzystwa Budownictwa Społecznego Sp. z o.o..

§ 11

1. Wszyscy pracownicy PTBSu przed przystąpieniem do pracy w systemie tradycyjnym i systemie elektronicznym przetwarzającym dane osobowe lub zbiorami danych osobowych zostają poddani przeszkoleniu w zakresie ochrony danych osobowych. Uczestnictwo w szkoleniu potwierdzają na karcie szkolenia (**załącznik nr 12**), która zostaje dołączona do akt osobowych.
2. Za organizację szkolenia odpowiada Administrator Danych Osobowych.
3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami Rozporządzenia, Ustawy o ochronie danych osobowych oraz wydawanymi na tej podstawie aktami wykonawczymi oraz instrukcjami obowiązującymi u administratora danych osobowych.
4. Zgodnie z wymogami Ustawy o ochronie danych osobowych pracownicy zostają zapoznani z przepisami z zakresu ww. ustawy w każdym przypadku istotnych zmian w przepisach dotyczących przetwarzania danych.
5. Szkolenie zostaje potwierdzone kartą szkolenia z zakresu RODO (przechowywane jest w aktach osobowych).
6. Administrator winien prowadzić rejestr odbytych szkoleń dla pracowników PTBSu zarówno dla nowo przyjętych pracowników jak i dla szkoleń okresowych. Wzór rejestru określa **załącznik nr 13** do niniejszej polityki.
7.

§ 12

1. Administrator Danych Osobowych ma obowiązek monitorowania zastosowanych środków ochrony.
2. W ramach kontroli należy zwracać szczególną uwagę na:
   1) okresowe sprawdzanie kopii bezpieczeństwa pod względem przydatności do możliwości odtwarzania danych;
   2) kontrola właściwej częstotliwości zmiany haseł;
   3) skuteczność zastosowanych zabezpieczeń fizycznych, technicznych i organizacyjnych.
3. Administrator Danych ma obowiązek śledzić zagrożenia wewnętrzne i zewnętrzne z szczególnym uwzględnieniem przepisów prawa oraz współpracować z Inspektorem Danych Osobowych.

§ 13

Naruszenie przetwarzania danych osobowych

1. W przypadku stwierdzenia prawdopodobieństwa wystąpienia naruszenia zasad ochrony danych osobowych, osoba która powzięła taką informację zobowiązana jest niezwłocznie powiadomić o swoich przypuszczeniach Administratora, w terminie nie później niż do końca dnia, w którym to wystąpiło.
2. Administrator dokonuje oceny zgłoszenia w zakresie wystąpienia ewentualnego naruszenia w szczególności:
   - zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy w Spółce,
   - może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
   - rozważa celowość i potrzebę powiadamia o zaistniałym naruszeniu Administratora danych,
   - nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza PTBS w Pszczynie.
3. Każdorazowo w przypadku naruszenia, które mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych, Administrator zgłasza bez zbędnej zwłoki fakt naruszenia

zasad ochrony danych osobowych w ośrodku organowi nadzorczemu, tj. nie później niż w terminie 72 godzin po stwierdzeniu naruszenia (po stwierdzeniu, że doszło do naruszenia).

4. Jeżeli ryzyko naruszenia praw i wolności okazuje się wysokie, Administrator powinien zawiadomić o incydencie także osobę, której dane dotyczą.
5. Administrator dokumentuje wszelkie czynności podjęte w ramach naruszenia przetwarzania danych osobowych, zgodnie z procedurą postępowania w przypadku naruszeń, który określa **załącznik nr 14** do Polityki Bezpieczeństwa.
6. Rejestr naruszeń sporządzony w formie elektronicznej prowadzi Inspektor Ochrony Danych Osobowych (**załącznik 14a**).
7. Do najważniejszych zagrożeń należą:
   - przechwycenie informacji - naruszenie poufności,
   - modyfikacja informacji - naruszenie integralności,
   - zniszczenie informacji - naruszenie dostępności,
   - blokowanie dostępu do informacji - naruszenie dostępności,
   - całkowitej utraty danych,
   - częściowej utraty danych,
   - uszkodzenia danych podczas przetwarzania,
   - celowego wprowadzania błędnych danych przez osoby nieuprawnione,
   - wejścia w posiadanie danych przez osoby nieuprawnione,
   - różne inne zagrożenia
8. Podział zagrożeń.
   - zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych.
   - zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.
   - zagrożenia zamierzone, świadome i celowe - najpoważniejsze zagrożenia, naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na: nieuprawniony

dostęp do systemu z zewnątrz (włamanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych składników systemu.

9. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to głównie:
   - sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
   - niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,
   - awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,
   - pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
   - jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
   - nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
   - stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
   - nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie,
   - ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń,
   - praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych - np. praca przy komputerze lub w sieci osoby, która nie jest

formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.,

- ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki", itp.,
- podmieniono lub zniszczono nośniki z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane osobowe,
- rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.).

Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, nośnikach elektronicznych w formie niezabezpieczonej itp.

§ 14
Powierzenie przetwarzania danych

1. Administrator może powierzyć przetwarzanie danych osobowych podmiotowi zewnętrznemu, pod warunkiem zawarcia z nim stosownej pisemnej określającej w szczególności zakres i cel przetwarzania danych. Umowa musi określać również zakres odpowiedzialności podmiotu zewnętrznego z tytułu niewykonania lub nienależytego wykonania umowy oraz sposobu jej rozwiązania. Wzór umowy powierzenia stanowi **załącznik nr 15 a** do niniejszej Polityki bezpieczeństwa**.** Ze względów organizacyjnych dopuszcza się prowadzenie rejestru przez poszczególne działy Administratora, które nadzorują realizację zawartych umów powierzenia. Administrator przyjmuje umowy przetwarzania danych osobowych podmiotu zewnętrznego (**załącznik nr 15**),
   zaś rejestr umów powierzenia określa **załącznik nr 16**
2. Administrator przed zawarciem umowy powierzenia ma obowiązek sprawdzić stan zabezpieczeń i poziom ochrony przetwarzania danych osobowych określony przez podmiot zewnętrzny i zapewnia sobie możliwość kontroli stanu przetwarzania

powierzonych danych w trakcie trwania umowy.

3. Niniejszy punkt nie ma zastosowania do przekazywania danych podmiotom upoważnionym do ich przetwarzania na mocy przepisów prawa, w tym szczególności ZUS, Prokuraturze, Policji, Sądom, Komornikom itp.

§ 15
Rejestr czynności przetwarzania

1. Zgodnie z Art. 30 RODO Administrator prowadzi rejestr czynności przetwarzania danych osobowych, który stanowi **załącznik nr 17** do Polityki bezpieczeństwa.
2. W przypadku przetwarzania danych w imieniu i na rzecz innego Administratora z użyciem powierzonych przez niego danych, administrator występuje w roli Podmiotu przetwarzającego i zgodnie z Art. 30 ust. 2 RODO prowadzi Rejestr kategorii czynności przetwarzania.

§ 16
Audyty

1. Zgodnie z art. 32 RODO, Administrator powinien regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.
2. W tym celu Administrator stosuje okresowe audyty prowadzone wewnętrznie przez IOD lub przez podmiot zewnętrzny, któremu zostanie zlecone przeprowadzenie audytu.
3. Celem audytów jest ocena, czy ochrona danych osobowych jest skutecznie realizowana i funkcjonuje zgodnie z wymaganiami RODO. Audyty prowadzone są w sposób obiektywny i bezstronny.
4. Audyty powinny być przeprowadzane raz w roku lub częściej jeżeli wymaga tego sytuacja (doszło do zmian organizacyjnych, zmian zabezpieczeń, zmian systemów informatycznych, incydentów, które mogły mieć wpływ na zabezpieczenia i innych zdarzeń mających wpływ na przetwarzanie danych osobowych).
5. Wyniki audytu określone są w postaci protokołu kontrolnego lub protokołu z audytu, który stanowi **załącznik nr 18** do Polityki bezpieczeństwa.

§ 17
Analiza ryzyka

Ocena skutków jest formalną, procedurą do przeprowadzenia w przypadkach określonych w Art. 35 RODO, w tym, w przypadku wysokiego poziomu ryzyka naruszenia praw i wolności osób fizycznych. W tym celu Administrator przeprowadza analizę ryzyka aby ocenić jego poziom i podjąć decyzję o konieczności przeprowadzenia oceny skutków. Przeprowadzenie analizy ryzyka może być również wykonane, nawet jeżeli Administrator nie ma takiego obowiązku, na potrzeby wykazania rozliczalności spełnienia wymagań RODO.W związku z obowiązkiem wyznaczenia Inspektora Ochrony Danych – ocena skutków musi być wykonana z jego współudziałem. Analiza ryzyka stanowi **załącznik nr 19**.

§ 18
Postanowienia końcowe

1. Wszyscy pracownicy zobowiązani są do zapoznania się z niniejszym dokumentem oraz do stosowania zawartych w nich reguł.
2. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.
3. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która wobec naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym Administratora Danych Ososbowych.
4. Kara dyscyplinarna orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby, zgodnie z Ustawą o ochronie danych osobowych oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
5. W sprawach nieuregulowanych w niniejszym dokumencie mają zastosowanie przepisy Rozporządzenia oraz Ustawy o ochronie danych osobowych.

6. Integralną częścią Polityki Bezpieczeństwa stanowią jej załączniki.
7. Polityka Bezpieczeństwa wchodzi w życie z dniem jej podpisania przez Zarząd i obowiązuje do czasu jej zmiany lub uchylenia.