Towarzystwo Budownictwa Społecznego Spółka z o.o. w Grajewie
ul. Konstytucji 3 Maja 27, 19-200 Grajewo
Sąd Rejonowy w Białymstoku XII Wydział Gospodarczy KRS 0000030421
NIP 719-13-87-142 Kapitał zakładowy 5 059 500,00zł
www.tbs.grajewo.pl
biuro@tbs.grajewo.pl

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH W TOWARZYSTWIE BUDOWNICTWA SPOŁECZNEGO SP. Z O.O. W GRAJEWIE

I. POSTANOWIENIA OGÓLNE

II. INSPEKTOR OCHRONY DANYCH

III. ZASADY PRZETWARZANIA - POSTANOWIENIA OGÓLNE

IV. ZASADY PRZETWARZANIA I OCHRONY DANYCH

V. POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

VI. ZBIERANIE DANYCH OSOBOWYCH

VII. GOTOWOŚĆ DO REALIZACJI UPRAWNIEŃ OSÓB, KTÓRYCH DANE SĄ PRZETWARZANE

VIII. NARUSZENIA OCHRONY DANYCH

IX. INWENTARYZACJA ZASOBÓW INFORMATYCZNYCH

X. OCENA RYZYKA I WYBÓR ZABEZPIECZEŃ

XI. REALIZOWANIE OBOWIĄZKÓW INFORMACYJNYCH

XII. MONITOROWANIE I SPRAWDZANIE

Rozdział 1.
POSTANOWIENIA OGÓLNE

§ 1

Towarzystwo Budownictwa Społecznego Sp. z o.o. w Grajewie działając na podstawie 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, ustanawia „Politykę Bezpieczeństwa".

§ 2

Polityka Bezpieczeństwa w TBS Sp. z o.o. w Grajewie jest zbiorem zasad i reguł obowiązujących przy zbieraniu, przetwarzaniu oraz wykorzystywaniu danych osobowych we wszystkich zbiorach administrowanych przez TBS Sp. z o.o. w Grajewie.

§ 3

Każda osoba, mająca dostęp do danych osobowych przetwarzanych w spółce jest zobowiązana do zapoznania się z niniejszym dokumentem.

Rozdział 2.
INSPEKTOR DANYCH OSOBOWYCH

§ 4

Zgodnie z art. 37 Rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. TBS Sp. z o.o. w Grajewie, działając jako Administrator Danych Osobowych (dalej jako „ADO") jest odpowiedzialny za realizację obowiązków wskazanych w niniejszej polityce.

ADO powołuje Inspektora Ochrony Danych, który będzie bezpośrednio realizował zadania w jego imieniu, ze szczególnym uwzględnieniem szacowania ryzyka oraz rozpatrywania naruszeń ochrony danych (w oparciu o procedurę wskazaną w Załączniku nr 1).
Szczegółowy zakres czynności Inspektora Ochrony Danych uregulowany jest w ramach nadawanego upoważnienia, którego wzór stanowi Załącznik nr 10 oraz według niniejszej Polityki Bezpieczeństwa.

§ 5

Ponadto nieuregulowane w niniejszej Polityce Bezpieczeństwa obowiązki Inspektora Ochrony Danych reguluje art. 39 Rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r.

§ 6

Inspektor Ochrony Danych ponadto odpowiadać będzie za kontrolowanie Spółki w zakresie stosowania zasad ochrony danych osobowych.

Rozdział 3.
ZASADY PRZETWARZANIA - POSTANOWIENIA OGÓLNE

§ 7

Osoby, które przetwarzają w spółce dane osobowe, muszą posiadać pisemne upoważnienie do przetwarzania danych nadane przez Administratora na wniosek Inspektora Ochrony Danych (Załącznik nr 5 do niniejszego dokumentu) oraz podpisać oświadczenie o zachowaniu poufności tych danych (Załącznik nr 2 do niniejszego dokumentu).

§ 8

Każda osoba posiadająca upoważnienie do przetwarzania danych osobowych posiada swój unikalny identyfikator oraz hasło pozwalające na zalogowanie się do systemu informatycznego, w którym przetwarzane są dane osobowe. Techniczne wymagania, jakie musi spełniać hasło zostały określone w odrębnym dokumencie „Instrukcja zarządzania systemem informatycznym".

§ 9

Inspektor Ochrony Danych prowadzi ewidencję osób dopuszczonych do pracy, z którymi może łączyć się dostęp do danych osobowych (Załącznik nr 3 do niniejszego dokumentu).

§ 10

Wszystkie budynki, pomieszczenia i części pomieszczeń, w których znajdują się dane osobowe stanowią obszar przetwarzania danych osobowych.

§ 11

Obszar przetwarzania danych osobowych objęty jest ochroną fizyczną w celu zabezpieczenia danych przed udostępnieniem osobom nieupoważnionym, wprowadzeniem zmian przez osobę nieupoważnioną, zabraniem przez osobę nieupoważnioną, uszkodzeniem lub zniszczeniem wskutek działania czynników naturalnych lub będących wynikiem ludzkiej działalności.

§ 12

Inspektor Ochrony Danych prowadzi wykaz budynków, pomieszczeń i części pomieszczeń stanowiących obszar przetwarzania danych osobowych stanowiący Załącznik nr 4 do niniejszego dokumentu.

Rozdział 4.
ZASADY PRZETWARZANIA I OCHRONY DANYCH

§ 13

Dokumenty zawierające dane osobowe przechowywane w formie papierowej, upoważnione osoby przechowują w obszarze przetwarzania danych w szafach zamykanych na klucz.

§ 14

Pracownik w momencie zakończenia pracy zamyka wszystkie drzwi szaf i szuflad służące do przechowywania danych osobowych, upewniając się, że osoby nieupoważnione nie będą w stanie dostać się do wskazanych danych.

§ 15

W przypadku konieczności dostępu do obszaru przetwarzania osób, nieposiadających upoważnienia, o jakim mowa w § 7, które muszą dokonać doraźnych prac o charakterze serwisowym (sprzątanie) lub innym, podpisują oni oświadczenie o zachowaniu poufności, chyba, że czynności odbywają się pod nadzorem osoby upoważnionej do przetwarzania danych.

§ 16

Pracownik w momencie zakończenia pracy upewnia się, czy wszystkie drzwi i okna w pomieszczeniach obszaru przetwarzania danych osobowych zostały prawidłowo zamknięte.

§ 17

Zakazuje się wynoszenia poza obszar przetwarzania danych osobowych bez zezwolenia materiałów zawierających dane osobowe.

§ 18

Inspektor Danych Osobowych jest zobowiązany do bieżącego nadzoru nad stosowaniem zabezpieczeń.

§ 19

Pracownicy zatrudnieni przy przetwarzaniu danych osobowych są zobowiązani do stosowania zabezpieczeń na swoich stanowiskach pracy.

§ 20

Inspektor Ochrony Danych prowadzi Rejestr czynności przetwarzania, stanowiący Załącznik nr 7.

§ 21

Przetwarzanie danych osobowych w Spółce dopuszczalne jest wyłącznie, gdy:
- jest niezbędne do zrealizowania uprawnień i spełnienia obowiązków wynikających z przepisów szczegółowych powszechnie obowiązujących aktów prawnych mających zastosowanie w działalności Spółki;
- jest konieczne do realizacji zawartej umowy lub przygotowania do jej zawarcia;
- osoba, której dane dotyczą wyrazi na to zgodę;
- jest niezbędne do wykonania określonych prawem zadań dla dobra publicznego;
- jest niezbędne dla dochodzenia roszczeń z tytułu umowy zawartej na piśmie;
- powierzone zostało Spółce w drodze umowy zawartej na piśmie.

§ 22

Przetwarzanie danych osobowych przez Spółkę jest dopuszczalne wyłącznie w zakresie jaki określają przepisy szczegółowe powszechnie obowiązujących aktów prawnych mających zastosowanie w działalności Spółki, uregulowania wewnętrzne Spółki oraz indywidualne umowy zawarte na piśmie z podmiotami zewnętrznymi, które powierzyły Spółce lub którym Spółka powierzyła przetwarzanie danych osobowych.

§ 23

Pracownicy zatrudnieni przy przetwarzaniu danych osobowych są zobowiązani do stosowania przyjętych w Spółce środków organizacyjnych i technicznych, zapewniających ochronę przetwarzania danych, w szczególności przed ich udostępnieniem, kradzieżą, uszkodzeniem lub zniszczeniem przez osoby nieupoważnione.

§ 24

Pracownicy zatrudnieni przy przetwarzaniu danych osobowych są zobowiązani do przechowywania danych osobowych we właściwych zbiorach, nie dłużej niż jest to niezbędne dla osiągnięcia celu ich przetwarzania.

§ 25

W przypadku konieczności zniszczenia papierowych dokumentów zawierających dane osobowe, ich zniszczenie dokonuje się poprzez użycie niszczarki. Następuje to po osiągnięciu celu przetwarzania danych osobowych. Postępowanie w zakresie niszczenia danych osobowych ustala Inspektor Ochrony Danych.

Rozdział 5.
POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

§ 26

W przypadku konieczności przekazania danych osobowych - zarówno w formie papierowej jak i elektronicznej - do podmiotu, który ma realizować cele wskazane przez Spółkę, uprzednio zawiera się umowę powierzenia przetwarzania, stanowiącą Załącznik nr 8 do niniejszego dokumentu.

Rozdział 6.
ZBIERANIE DANYCH OSOBOWYCH

§ 27

Dane osobowe są przetwarzane w Spółce w postaci zbiorów danych.

§ 28

Inspektor Ochrony Danych prowadzi:
1. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.
2. Opis struktury zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych i powiązań między nimi.

3. Sposób przepływu danych pomiędzy poszczególnymi systemami.
Wykaz stanowi Załącznik nr 6 niniejszego dokumentu.

Rozdział 7.
GOTOWOŚĆ DO REALIZACJI UPRAWNIEŃ OSÓB, KTÓRYCH DANE SĄ PRZETWARZANE

§ 29

TBS Sp. z o.o. w Grajewie zapewnia możliwość:
a) sprostowania (poprawienia) danych;
b) usunięcia danych przetwarzanych bezpodstawnie;
c) ograniczenia przetwarzania danych;
d) dostępu do treści przetwarzanych danych osobowych - w formie udostępnienia bezpłatnej kopii danych osobowych (w formie elektronicznej lub papierowej);
e) przeniesienia danych do innego administratora danych lub Państwa (w zakresie określonym w art. 20 RODO);
chyba, że przepis ustawy zwalnia Spółkę z tego obowiązku lub żądanie osoby, której dane są przetwarzane jest ewidentnie nieuzasadnione lub nadmierne.

§ 30

W przypadku uznania żądania za ewidentnie nieuzasadnione lub nadmierne należy uzasadnić odmowę realizacji żądania wskazując powody przemawiające za przyjęciem takiej kwalifikacji i w formie pisemnej przekazać uzasadnienie osobie wnoszącej żądanie informując o możliwości wniesienia skargi do organu nadzorczego.

§ 31

W przypadku tych informacji, które są przetwarzane przy użyciu środków elektronicznych na podstawie zgody lub umowy, TBS Sp. z o.o. w Grajewie przetwarza je w formie pozwalającej na przekazanie i odczyt przez innego administratora - jeżeli osoba, której dane dotyczą skorzysta z uprawnienia do przeniesienia dostarczonych przez nią danych.

§ 32

Dane osobowe przetwarzane przez Spółkę udostępniane są wyłącznie na pisemny, umotywowany wniosek, chyba, że przepis innej ustawy, na który powoła się proszący o udostępnienie danych, stanowi inaczej.

§ 33

Rozpatrywane są jedynie wnioski zawierające informacje, umożliwiające wyszukanie żądanych danych osobowych w zbiorze.

§ 34

Wnioski o udostępnienie danych rozpatrywane są przez Inspektora Ochrony Danych.

Rozdział 8.
NARUSZENIA OCHRONY DANYCH

§ 35

Inspektor Ochrony Danych działając w imieniu TBS Sp. z o.o. w Grajewie informuje każdą osobę upoważnioną o potencjalnych możliwych naruszeniach ochrony danych i obowiązku ich niezwłocznego komunikowania w formie wyciągu. Opracowana została „Instrukcja postępowania w sytuacji naruszenia ochrony danych" stanowiąca Załącznik nr 9 do niniejszego dokumentu.

§ 36

W przypadku pozyskania informacji z jakiegokolwiek źródła o potencjalnym naruszeniu ochrony danych, Inspektor Ochrony Danych natychmiast podejmuje niezbędne środki w celu ustalenia, czy konkretne zdarzenie miało miejsce, a następnie, czy stanowiło ono naruszenie ochrony danych osobowych. Na tyle, na ile jest to możliwe należy podjąć działania, które ograniczą rozmiar i dotkliwość naruszenia dla osób, których danych ono dotyczyło.

§ 37

Z chwilą stwierdzenia naruszenia, Inspektor Ochrony Danych niezwłocznie dokonuje jego klasyfikacji.

§ 38

Każde stwierdzone naruszenie musi zostać odnotowane w wewnętrznym rejestrze naruszeń (wzór stanowi Załącznik nr 10).

§ 39

1. W przypadku stwierdzenia naruszenia ochrony danych osobowych Inspektor Ochrony Danych dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych.
2. W każdej sytuacji, w której zaistnienie naruszenia mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych, Inspektor Ochrony Danych zgłasza fakt naruszenia zasad ochrony danych organowi nadzorczemu bez zbędnej zwłoki - jeżeli to wykonalne, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia.
3. Jeżeli ryzyko naruszenia praw i wolności jest wysokie Administrator zawiadamia o incydencie także osobę, której dane dotyczą.

Rozdział 9.
INWENTARYZACJA ZASOBÓW INFORMATYCZNYCH

§ 40

Inspektor Ochrony Danych wykonuje i prowadzi na bieżąco inwentaryzację sprzętu wykorzystywanego do przetwarzania informacji mogących stanowić dane osobowe (inwentaryzacja zasobów informatycznych) oraz oprogramowania. Inwentaryzacja polega na ustaleniu w stopniu wyczerpującym i kompletnym:

a) jakie urządzenia są wykorzystywane do przetwarzania danych osobowych;
b) jakie oprogramowanie jest wykorzystywane do przetwarzania danych osobowych;
c) kategorii informacji przetwarzanych na konkretnych, odnotowanych co do tożsamości urządzeniach;
d) miejscu ich przechowywania;
e) osobach, które mogą mieć dostęp do tych urządzeń.

Inwentaryzacja zasobów informatycznych zapisywania jest w formie dokumentu, którego wzór stanowi Załącznik nr 11 do niniejszej Polityki Bezpieczeństwa.

Rozdział 10.
OCENA RYZYKA I WYBÓR ZABEZPIECZEŃ

§ 41

Inspektor Ochrony Danych zarządza przeprowadzenie wstępnej analizy ryzyka, która polega na przyporządkowaniu do wyników inwentaryzacji z Rozdziału 9 niniejszego dokumentu potencjalnych zagrożeń dla bezpieczeństwa danych osobowych wraz z zapisem i uzasadnieniem decyzji o konkretnych działaniach związanych z zabezpieczeniem informacji.

§ 42

Inspektor Ochrony Danych zobowiązany jest do uwzględnienia możliwości nieuprawnionego lub przypadkowego działania na danych osobowych w sposób:
a) zniszczenia;
b) utraty;
c) zmodyfikowania;
d) nieuprawnionego ujawnienia;
e) nieuprawionego dostępu.

§ 43

Analiza ryzyka wykonywana jest z perspektywy potencjalnych negatywnych skutków dla osób, których dane osobowe są przetwarzane w ramach prowadzonej działalności.

Rozdział 11.
REALIZOWANIE OBOWIĄZKÓW INFORMACYJNYCH

§ 44

Inspektor Ochrony Danych działając na rzecz TBS Sp. z o.o. w Grajewie przekazuje każdej osobie, której dane są przetwarzane informacje, o których mowa w § 31, chyba, że przepis ustawy przewiduje zwolnienie z tego obowiązku.

Rozdział 12.
MONITOROWANIE I SPRAWDZANIE

§ 45

Inspektor Ochrony Danych odpowiedzialny jest za przestrzeganie przyjętych procedur ochrony danych osobowych. Posiada uprawnienia do sprawdzeń przestrzegania przez osoby upoważnione do przestrzegania zasad bezpieczeństwa przetwarzania danych osobowych. Sprawdzenia odbywają się niezapowiedzianie względem osób kontrolowanych.

Sprawdzenia odbywają się m.in. w sposób: wizytacji i oględzin na stanowisku pracy ze szczególnym uwzględnieniem stanu i sposobu korzystania z mebli biurowych służących do przechowywania dokumentów lub elektronicznych nośników informacji, sprawdzeniu sposobów korzystania z urządzeń elektronicznych służących do przetwarzania danych osobowych.

§ 46

W przypadku dokonywania aktualizacji należy sprawdzić, czy zachodzi konieczność dokonania ponownego szacowania ryzyka, o której mowa w Rozdziale 10. W przypadku wątpliwości co do odpowiedzialności zastosowanych środków bezpieczeństwa zaleźy dokonać ponownej oceny ryzyka.

§ 47

Inspektor Ochrony Danych przynajmniej raz na miesiąc sprawdza wytyczne i rekomendacje wydawane przez Organ Nadzorczy oraz Europejską Radę Ochrony Danych Osobowych poprzez sprawdzenie treści zamieszczanych na oficjalnych stronach internetowych. Zapisane wytyczne i rekomendacje przechowywane są w formie elektronicznej w katalogu na głównym komputerze służbowym.

§ 48

Niniejszy dokument wchodzi w życie z dniem 25 maja 2018 roku.

PREZES ZARZĄDU
TBS Sp. z o.o. w Grajewie
Tomasz Strózik

Towarzystwo Budownictwa Społecznego Sp. z o.o.
w Grajewie
19-200 Grajewo, ul. Konstytucji 3 Maja 27
NIP 719-13-87-142 REGON 450711988