POLITYKA BEZPIECZEŃSTWA

Regionalne Wąbrzeskie Towarzystwo Budownictwa Społecznego Spółka z o.o.

15.05.2018 r.
Wąbrzeźno

§ 1
Podstawa prawna i cel opracowania dokumentu

1. Niniejszy dokument został stworzony w celu wdrożenia wymogów określonych w powszechnie obowiązujących przepisach prawa, w tym nade wszystko w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) z dnia 27 kwietnia 2016 r.
2. Przedmiotowy akt należy odczytywać łącznie z pozostałym wewnętrznymi regulacjami takimi jak:
   a) Rejestr czynności przetwarzania danych osobowych (który to dokument określa w szczególności kategorie przetwarzanych danych, podstawę ich przetwarzania, cel, kategorie odbiorców danych);
   b) Instrukcja zarządzania system informatycznym (której celem jest wzmocnienie poziomu ochrony danych przetwarzanych w inny sposób niż w formie tradycyjnej).

§ 2
Definicje

1) **Administrator danych** – Regionalne Wąbrzeskie Towarzystwo Budownictwa Społecznego Spółka z o.o., z siedzibą ul. Kętrzyńskiego 121A, 87 – 200 Wąbrzeźno, wpisaną do rejestru przedsiębiorców KRS 0000122375, NIP 878-10-54-092 (dalej również jako RW TBS).

2) **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (osoby, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne),

3) **przetwarzanie danych osobowych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie udostępnianie i usuwanie, a zwłaszcza te które wykonuje się w systemach informatycznych,

4) **usuwanie danych** – zniszczenie danych osobowych

5) **anonimizacja –** modyfikacja danych, na skutek której brak jest możliwości ustalenia tożsamości osoby, której dane dotyczą,

6) **użytkownik** - rozumie się przez to upoważnionego przez Administratora danych, wyznaczonego do przetwarzania danych osobowych Pracownika;
7) **pracownik** - należy przez to rozumieć osobę zatrudnioną przez Administratora danych w formie umowy o pracę lub umowy cywilno-prawnej lub inną osobę współpracującą.

§ 3
Cel polityki bezpieczeństwa

Celem Polityki Bezpieczeństwa przetwarzania danych osobowych w Spółce RW TBS jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania informacji zawierających Dane osobowe, a przede wszystkim zapewnienie ochrony przetwarzanych Danych osobowych przed wszelkiego rodzaju zagrożeniami, tak zewnętrznymi jak i wewnętrznymi.

§ 4
Zakres stosowania Polityki Bezpieczeństwa

W ramach zabezpieczenia danych osobowych ochronie podlegają w szczególności:

a) sprzęt komputerowy – serwer, komputery osobiste (w tym przenośne) i inne urządzenia zewnętrzne,
b) oprogramowanie (w tym oprogramowanie działające w systemie software as service)
c) Dane osobowe zapisane na informatycznych nośnikach danych oraz dane przetwarzane w systemach informatycznych,
d) hasła użytkowników,
e) bazy danych i kopie zapasowe,
f) wydruki,
g) związana z przetwarzaniem danych dokumentacja papierowa.

§ 5
Podstawowe zasady ochrony Danych osobowych

Administrator danych powinien realizować następujące zasady:

a) **Legalności** – przetwarzanie Danych osobowych może się odbywać wyłącznie, gdy zaistnieje co najmniej jedna z przewidzianych prawem przesłanek (np. zgoda osoby od której dane pochodzą);

b) **Celowości** – aby dane mogły być przetwarzane, musi istnieć ku temu konkretny, wyraźny i prawnie uzasadniony cel. Jeżeli przetwarzanie służy

różnym celom, potrzebna jest zgoda/podstawa na wszystkie cele. Cel zbierania danych powinien być zakomunikowany osobie, której dane dotyczą jeszcze przed faktycznym zebraniem od niej Danych osobowych;

c) **Adekwatności** – przetwarzając dane Administrator powinien kierować się zasadą minimalizacji danych – powinien on przetwarzać tylko takie dane, które są mu niezbędne ze względu na cel ich zbierania;

d) **Merytorycznej poprawności** – Administrator danych jest zobowiązany do tego, aby dane przez niego zbierane były poprawne i w razie potrzeby uaktualniane. Powinien oceniać wiarygodność źródła pozyskania danych oraz wdrożyć sposób weryfikowania prawdziwości przetwarzanych danych;

e) **Czasowości** – zasada ograniczenia przechowywania danych – obowiązek przechowywania danych osobowych przez okres nie dłuższy niż jest niezbędne do celów, w których dane te są przetwarzane. Obowiązkiem Administratora jest to, by każdorazowo dokonywać indywidualnej oceny, czy w dalszym ciągu zachodzi konieczność przetwarzania Danych osobowych.

f) **Integralności i poufności danych** – forma przetwarzania danych osobowych powinna być tak zabezpieczona za pomocą odpowiednich środków technicznych lub organizacyjnych, by zapewniała adekwatne bezpieczeństwo danych osobowych, w tym ochronę przed niezgodnym z prawem przetwarzaniem, przypadkową utratą, zniszczeniem lub uszkodzeniem;

g) **Rozliczalności –** Administrator danych powinien móc wykazać, iż postępuje zgodnie z zasadami dotyczącymi przetwarzania danych osobowych;

h) **Przejrzystości** – informacje kierowane do osoby, której dane dotyczą, związane z przetwarzaniem jej danych, mają być dla niej łatwo dostępne, zrozumiałe, oraz sformułowane jasnym i prostym językiem. Osobom fizycznym należy uświadomić ryzyka, zasady, zabezpieczenia i prawa związane z przetwarzaniem danych osobowych oraz sposoby ich wykonywania.

§ 6
Obszar przetwarzania danych osobowych

1. Przetwarzanie Danych osobowych przez Administratora danych odbywa się:

- przy wykorzystaniu systemów informatycznych oraz
- poza systemem w wersji papierowej

2. Za obszar przetwarzania danych należy rozumieć obszar, w którym wykonywana jest choćby jedna z czynności przetwarzania danych osobowych.
3. Obszar przetwarzania Danych osobowych został określony w Załączniku nr 1 do Polityki bezpieczeństwa.

§ 7
Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych

1. Zabezpieczenia organizacyjne :

a) sporządzono i wdrożono Politykę Bezpieczeństwa;
b) sporządzono i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania Danych osobowych;
c) do przetwarzania Danych osobowych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez Administratora danych bądź osobę przez niego upoważnioną;
d) stworzono stale uaktualniany rejestr osób upoważnionych do przetwarzania Danych osobowych;
e) stworzono procedurę postępowania w sytuacji naruszenia ochrony Danych osobowych;
f) osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony Danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego;
g) osoby zatrudnione przy przetwarzaniu Danych osobowych obowiązane zostały do zachowania ich w tajemnicy;
h) Dane osobowe są powierzane do przetwarzania wyłącznie profesjonalnym, zaufanym podmiotom. Obowiązki podmiotów uczestniczących jako procesor w przetwarzaniu danych są określane w umowach powierzenia;
i) Administrator ściśle przestrzega obowiązków, wynikających z umów, na mocy których powierzono mu dane osobowe do przetwarzana;
j) Administrator dostrzega w swojej działalności dane wymagające szczególnej ochrony:
   - danych o stanie zdrowia personelu;
   - informacje zawarte w orzeczeniach sądowych lub administracyjnych;
   - danych osób skazanych, skierowanych do realizacji określonych prac.

   W stosunku do tych danych Administrator podejmuje dodatkowe środki, służące zachowaniu poufności i integralności danych, w tym nade wszystko:

- przetwarzanie wskazanych danych możliwe jest w ściśle uzasadnionych przypadkach. W sytuacji, gdy Administrator wejdzie w posiadanie danych, co do których brak podstaw do przetwarzania (np. nieuzasadnione dostarczenie dokumentacji medycznej przez lokatora), dane te powinny zostać uznane za dane niepożądane, a w ślad za tym zwrócone wraz z uzasadnieniem;
- do przetwarzania wskazanych danych mogą być dopuszczone wyłącznie osoby upoważnione (upoważnienia w tym zakresie powinny być ściśle limitowane, dostosowane do faktycznych obowiązków. Złą praktyką byłoby nadanie wszystkim pracownikom równych poziomem upoważnień);
- wskazane dane powinny być przechowywane w taki sposób, ażeby dostęp do nich posiadały wyłącznie osoby upoważnione. Ponadto, z uwagi na charakter danych, powinny być przechowywane w pomieszczeniach, do których w standardowych sytuacjach nie mają zupełnie wstępu osoby postronne (typu listonosz, petenci, inne).

2. Zabezpieczenia techniczne:

a) przetwarzanie Danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych, a w szczególności:
- budynek objęty jest profesjonalnym systemem alarmowym,
- dostęp do pomieszczeń, w których przetwarzane są Dane osobowe możliwy jest wyłącznie dla osób upoważnionych,
- klucze do tych pomieszczeń posiadają wyłącznie osoby uprawnione,
- przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są Dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych,
- w przedsiębiorstwie Administratora danych obowiązuje tzw. zasada czystego biurka, z której wynika zakaz eksponowania Danych osobowych w obrębie stanowiska pracy, w szczególności w przypadku jego czasowego lub długotrwałego opuszczenia,
- w przedsiębiorstwie Administratora danych obowiązuje tzw. zasada czystego ekranu oraz czystego pulpitu, z której wynika zakaz eksponowania Danych osobowych w obrębie monitora, w szczególności w przypadku jego czasowego lub długotrwałego opuszczenia,
- Dane osobowe są udostępniane tylko w sytuacji, gdy istnieje ku temu niezbędna podstawa (najczęściej przepis prawa lub zgoda osoby, od której dane pochodzą),
- w konsekwencji, osoby postronne nie mają możliwości uzyskania dostępu do danych osobowych w żadnej postaci,
- nie zachodzi również ryzyko nielegalnego przetwarzania danych;

b) dokumenty i nośniki informacji zawierające Dane osobowe, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonując takiej ich modyfikacji, która nie pozwoli na odtworzenie ich treści, aby po dokonaniu usunięcia danych niemożliwa była identyfikacja osób.
c) dostęp do systemu operacyjnego komputerów, w których przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelniania z wykorzystaniem identyfikatora użytkownika oraz hasła;
d) ponadto, dostęp do oprogramowania, które służy do przetwarzania danych osobowych zabezpieczony jest za pomocą procesu uwierzytelniania z wykorzystaniem identyfikatora użytkownika oraz hasła;
e) identyfikatory i hasła, o których mowa w podpunkcie c) oraz d) nie są tożsame;
f) podstawowe oprogramowanie stosowane do przetwarzania danych osobowych gwarantuje zdolność do:

   - ciągłego zapewnienia poufności, integralności, dostępności i odporności danych,

   - szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego**;**

g) dokonywanie zmian w systemie (w tym instalowanie zewnętrznego oprogramowania) zastrzeżone jest dla administratora IT tj. szeregowy użytkownik nie jest w stanie samodzielnie tego rodzaju zmian wprowadzać;
h) na komputerach zainstalowane jest stale aktualizowane oprogramowanie antywirusowe oraz typu firewall;
i) w przypadku awarii sprzętowej lub oprogramowania, zgodnie z przyjętą procedurą następuje zgłoszenie do informatyka lub we wskazanych przypadkach do dostawcy oprogramowania.

§ 8
Obowiązki informacyjne i komunikacja

1. Administrator dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.

2. Administrator ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym: zamieszczenie na stronie internetowej informacji o uprawnieniach.

3. Administrator dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób. W tym celu, Administrator wprowadza w życie „Rejestr wniosków".

§ 9

Instrukcja postępowania w przypadku zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych

1. Instrukcja definiuje katalog zagrożeń i incydentów zagrażających bezpieczeństwu Danych osobowych oraz opisuje sposób reagowania na nie. Celem instrukcji jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa, ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.
2. Każdy pracownik w przypadku stwierdzenia zagrożenia lub naruszenia ochrony Danych osobowych, zobowiązany jest niezwłocznie poinformować Administratora danych.
3. Do typowych zagrożeń bezpieczeństwa Danych osobowych należą:
   a) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
   b) niewłaściwe zabezpieczenie sprzętu, oprogramowania przed wyciekiem, kradzieżą i utratą Danych osobowych,
   c) nieprzestrzeganie zasad ochrony Danych osobowych przez pracowników.
4. Do typowych incydentów bezpieczeństwa Danych osobowych należą:
   a) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
   b) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/ zagubienie danych),
   c) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie Danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).
5. W przypadku stwierdzenia wystąpienia zagrożenia, Administrator danych prowadzi postępowanie wyjaśniające w toku, którego:
   a) ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki,
   b) inicjuje ewentualne działania dyscyplinarne,
   c) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji zagrożeń w przyszłości,
   d) dokumentuje prowadzone postępowania.
6. W przypadku stwierdzenia incydentu (naruszenia) Administrator danych prowadzi postępowanie wyjaśniające w toku, którego:
   a) ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały,
   b) zabezpiecza ewentualne dowody,
   c) ustala osoby odpowiedzialne za naruszenie,
   d) podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody),
   e) inicjuje działania dyscyplinarne,

f) wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości,
g) dokumentuje prowadzone postępowania.

7. W przypadku naruszenia ochrony Danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je Prezesowi Urzędu Ochrony Danych Osobowych.
8. Obowiązek, o którym mowa w ust. 7 nie powstaje, jeżeli jest mało prawdopodobne, by odnotowany incydent skutkował ryzykiem naruszenia praw lub wolności osób fizycznych.
9. Zgodnie z literą prawa, zgłoszenie powinno zawierać:
   a) 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;
   b) imię i nazwisko oraz dane kontaktowe wyznaczonej u Administratora osoby, która będzie w stanie udzielić bardziej szczegółowych informacji;
   c) opis możliwych konsekwencje naruszenia ochrony Danych osobowych;
   d) opis zastosowanych lub proponowanych przez Administratora środków w celu zaradzenia naruszeniu ochrony Danych osobowych
10. W przypadku przekroczenia terminu 72 h, zgłoszenie musi zawierać precyzyjne określenie przyczyn opóźnienia.
11. Wszelkie podmioty, które przetwarzają Dane osobowe na zlecenie Administratora powinny zostać pouczone o obowiązku niezwłocznego informowania o wszelkich incydentach.

§ 10
Zadania Administratora Danych

1. Do najważniejszych obowiązków Administratora Danych należy:

a) organizacja bezpieczeństwa i ochrony Danych osobowych zgodnie z wymogami ustawy o ochronie danych osobowych,
b) zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki Bezpieczeństwa,
c) wydawanie i anulowanie upoważnień do przetwarzania Danych osobowych,
d) prowadzenie ewidencji osób upoważnionych do przetwarzania Danych osobowych,

e) prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony Danych osobowych, prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony Danych osobowych,
f) nadzór nad bezpieczeństwem Danych osobowych,
g) kontrola działań komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie Danych osobowych,
h) inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony Danych osobowych,
i) Zawiadamianie organu nadzoru w przypadkach przewidzianych prawem.

2. Zadania Administratora mogą wykonywać wszyscy wspólnicy spółki cywilnej łącznie, jak też każdy z nich z osobna. Brak jest przeciwwskazań prawnych, by obowiązki Administratora przydzielić tylko jednemu ze wspólników. Nie zwalnia to pozostałych wspólników z odpowiedzialności za prawidłowe, zgodne z prawem przetwarzanie Danych osobowych.

§ 11
Postanowienia końcowe

1. Administrator danych ma obowiązek zapoznać z treścią Polityki każdego pracownika.
2. Wszelkie zmiany niniejszego dokumentu będą publikowane w sposób zwyczajowo przyjęty u Administratora danych.

Załączniki:

1. Obszar przetwarzania Danych osobowych;
2. Wzór upoważnienia do przetwarzania Danych osobowych;
3. Wzór oświadczenia o zobowiązaniu się do zachowania poufności;
4. Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych.

Załącznik nr 1 - Obszar przetwarzania Danych osobowych

1. Dane osobowe przetwarzane są w siedzibie Administratora tj. przy ul. Kętrzyńskiego 121 A, 87-200 Wąbrzeźno;
2. Dostęp do danych jest ściśle ograniczony i podlega kontroli;
3. Dostęp do Elektronicznego Biura Obsługi Klienta (narzędzia informatycznego, dostępnego z poziomu strony www.rwtbs.wabrzezno.com, zakładka E-USŁUGI) możliwy jest wyłącznie dla osób wyposażonych w indywidualny identyfikator oraz hasło. Za pośrednictwem tego modułu udostępniane są wyłącznie podstawowe informacje dotyczące danej osoby. Z wykorzystaniem tego narzędzia nie są udostępniane żadne dane wrażliwe.
4. Decyzję o tym, który z pracowników uzyska dostęp do Danych osobowych oraz w jakim zakresie podejmuje Administrator Danych;
5. Kopie zapasowe przechowywane na sieciowym dysku zewnętrznym NAS oraz na jednej ze stacji roboczych (zawsze innej aniżeli dane źródłowe).

Załącznik nr 2 - Wzór upoważnienia do przetwarzania Danych osobowych

Wąbrzeźno, dnia ……..

Regionalne Wąbrzeskie Towarzystwo

Budownictwa Społecznego Spółka z o.o.

UPOWAŻNIENIE

do przetwarzania danych osobowych w zbiorach:
……
……
oraz danych powierzonych do przetwarzania przez podmioty zewnętrzne:
……
……

Imię i nazwisko osoby upoważnionej
……
Stanowisko służbowe/ funkcja:
……..……..
Data udzielenia upoważnienia: ……

Zakres upoważnienia:

- Przetwarzanie danych osobowych w formie papierowej
  TAK/NIE

- Przetwarzanie danych osobowych w systemach informatycznych
  TAK/NIE

  - Nazwa systemów informatycznych, do których pracownik otrzymuje dostęp:

    ……
    ……

Upoważnienie obejmuje uprawnienia do wykonywania następujących działań na danych osobowych:

- Wprowadzanie danych **TAK/NIE**
- Edycja danych **TAK/NIE**
- Usuwanie danych **TAK/NIE**
- Podgląd danych **TAK/NIE**

Osoba upoważniona zobowiązuje się do przetwarzania danych osobowych zgodnie z:

- powszechnie obowiązującymi przepisami - przede wszystkim zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) z dnia 27 kwietnia 2016 r.

- udzielonym upoważnieniem

- jak również obowiązującymi w RWTBS wewnętrznymi regulacjami w sprawie ochrony danych osobowych.

Podpis osoby otrzymującej upoważnienie:
……

Podpis osoby nadającej upoważnienie:
……

Data wygaśnięcia upoważnienia ……../Upoważnienie automatycznie wygasa w dniu zakończenia umowy o pracę/umowy o współpracy.

Załącznik nr 3 - Wzór oświadczenia o zobowiązaniu się do zachowania poufności

……., dnia ……..

Oświadczenie o zobowiązaniu się do zachowania poufności

Ja niżej podpisana/y . . . . . zamieszkała/y w . . . . . zatrudniona/y na stanowisku . . . . . zobowiązuję się zachować w tajemnicy informacje uzyskane w związku z przetwarzaniem danych osobowych w zbiorach:

……
……..…...

Uzyskane informacje zachowam w poufności zarówno w trakcie obowiązywania umowy, jak i po jej ustaniu.

…….……..
Podpis

Załącznik nr 4 - Wzór ewidencji osób upoważnionych do przetwarzania Danych osobowych

lp.	Dane osoby upoważnionej	Zakres upoważnienia	Daty udzielenia i wygaśnięcia upoważnienia