POLITYKA OCHRONY DANYCH OSOBOWYCH

ZWAŻYWSZY, ŻE:

i. w dniu 25 maja 2018 roku weszło w życie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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), zwane dalej „**RODO**" oraz ustawa z dnia 12 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r., poz. 1000);

ii. rozporządzenie nakłada na podmioty gospodarcze obowiązek dostosowania standardów przetwarzania danych osobowych do postanowień rozporządzenia;

Zarząd SHARE HOME SILESIA sp. z o.o. uchwałą z dnia 25.05.2018 r. postanowił przyjąć niniejszą Politykę Bezpieczeństwa Danych Osobowych, która wraz z załącznikami:

i. opisuje zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym dostępem;

iii. zapewnia zgodności przetwarzania danych osobowych w Spółce z przepisami RODO; oraz

iv. stanowi politykę ochrony danych osobowych w rozumieniu ww. rozporządzenia.

§ 1
DEFINICJE

1. Ilekroć w niniejszym dokumencie używa się następujących pojęć, mają one znaczenie nadane poniżej:

   1.1. **„Administrator" lub „Spółka"** – oznacza SHARE HOME SILESIA spółka z ograniczoną odpowiedzialnością z siedzibą w Katowicach, ul. Konduktorska 33, 40-155 Katowice, wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego pod nr KRS 0000658555, REGON: 366336021, NIP: 6342884703 o kapitale zakładowym w wysokości 13 815 000,00 złotych.

   1.2. **„Administrator Systemu Informatycznego" „ASI"** – oznacza osobę lub dział w strukturze Administratora lub podmiot zewnętrzny działający w imieniu Administratora i zajmujący się zarządzaniem systemem informatycznym, tj. m.in. nadzorowaniem pracy serwerów, zarządzaniem kontami użytkowników, instalowaniem oprogramowania, zapewnieniem bezpieczeństwa systemu i zgromadzonych danych, a także nadzorowaniem, wykrywaniem i usuwaniem nieprawidłowości w funkcjonowaniu systemu informatycznego Administratora oraz dokonywaniem instalacji, konfiguracji i napraw sprzętu.

   1.3. **„Polityka"** – oznacza niniejszą Politykę Ochrony Danych Osobowych wraz z załącznikami.

   1.4. **„RODO"** – oznacza 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 (ogólne rozporządzenie o ochronie danych) z dnia 27 kwietnia 2016 r. (Dz. Urz. UE.L Nr 119, str. 1).

   1.5. **„Dane Osobowe"** – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osoba, której dane dotyczą"). Pod pojęciem możliwej do zidentyfikowania osoby fizycznej rozumie się osobę, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie imienia i nazwiska, numeru identyfikacyjnego, danych o lokalizacji, identyfikatora internetowego lub jednego bądź kilku szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

1.6. **„Przetwarzanie Danych Osobowych”** – 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.

1.7. **„Podmiot Przetwarzający”** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora.

1.8. **„System informatyczny”** – oznacza zespół powiązanych funkcjonalnie i współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi wykorzystywanych w celu Przetwarzania Danych Osobowych.

1.9. „**Użytkownik**”– oznacza osobę mającą dostęp do zasobów systemu informatycznego i posiadającą upoważnienie Administratora do Przetwarzania Danych Osobowych.

1.10. „**Zbiór danych**” – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie; dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

1.11. **„Zgoda”**– oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

1.12. **„Odbiorca danych”** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania.

§ 2
CELE WPROWADZENIA POLITYKI

1. Niniejsza Polityka stanowi uregulowanie zasad przetwarzania Danych Osobowych w Spółce.
2. Celem wprowadzenia Polityki jest ustanowienie standardów i reguł postępowania pozwalających na wdrożenie obowiązków Administratora w zakresie ochrony Danych Osobowych, w szczególności poprzez ustanowienie zasad mających na celu:
   2.1. Przetwarzania Danych Osobowych w Spółce zgodnie z prawem;
   2.2. uniemożliwienie dostępu do Danych Osobowych osobom do tego nieupoważnionym;
   2.3. zabezpieczenie Danych Osobowych przed ich nieuprawnionym ujawnieniem, kradzieżą, zniszczeniem, uszkodzeniem lub innym bezprawnym pozyskaniem i wykorzystaniem.

§ 3
ZAKRES ZASTOSOWANIA POLITYKI

1. Niniejsza Polityka ma zastosowanie do wszystkich Zbiorów Danych Osobowych przetwarzanych przez Administratora, w szczególności do:
   1.1. Zbiorów Danych Osobowych prowadzonych zarówno w postaci elektronicznej, jak i w formie tradycyjnej (papierowej, pisemnej), w tym danych zgromadzonych na wszystkich istniejących Systemach informatycznych Administratora oraz ewentualnych Systemach informatycznych,

które zostaną wdrożone w przyszłości, bez względu na sposób utrwalenia Danych Osobowych i rodzaj nośników, na których zostały utrwalone;

1.2. Danych Osobowych, przetwarzanych przez Administratora w imieniu własnym, jak również danych przetwarzanych przez Administratora na podstawie umów o powierzenie przetwarzania danych osobowych;

1.3. Danych Osobowych przetwarzanych we wszystkich budynkach i pomieszczeniach Administratora.

2. Zakres podmiotowy obowiązywania Polityki obejmuje wszystkie osoby, bez względu na zajmowane stanowisko oraz charakter stosunku prawnego, w tym pracy lub świadczenia usług (włączając stażystów, praktykantów, uczniów, osoby podejmujące czynności na podstawie stosunku powołania oraz osoby wykonujące pracę na podstawie umowy zlecenia lub umowy o dzieło) i bez względu na miejsce wykonywania, a które mają dostęp do Danych Osobowych zbieranych, przetwarzanych oraz przechowywanych przez Administratora w związku z prowadzoną działalnością.

3. Osoby mające dostęp do Danych Osobowych zobowiązane są do stosowania środków określonych w niniejszej Polityce oraz aktach prawa powszechnego. Środki te pozostają wiążące także po ustaniu stosunku podstawowego, z którym wiązał się dostęp do Danych Osobowych.

§ 4
ZASADY PRZETWARZANIA DANYCH

1. System przetwarzania Danych Osobowych Administratora opiera się na następujących zasadach:

1.1. zgodności z prawem, rzetelności i przejrzystości Przetwarzania Danych Osobowych;

1.2. ograniczenia celu – tj. Przetwarzania Danych Osobowych w konkretnych, wyraźnie określonych i prawnie uzasadnionych celach;

1.3. minimalizacji danych – tj. przetwarzaniu wyłączenie tych Danych Osobowych, które są konieczne z uwagi na wskazany cel Przetwarzania;

1.4. prawidłowości – tj. podejmowania wszelkich rozsądnych działań, aby Dane Osobowe, które są nieprawidłowe w kontekście celów ich Przetwarzania, zostały niezwłocznie usunięte lub sprostowane;

1.5. ograniczenia przechowywania – tj. przechowywania Danych Osobowych przez okres nie dłuższy niż wynikający z celów Przetwarzania;

1.6. integralności i poufności – Przetwarzanie Danych Osobowych w sposób zapewniający odpowiednie bezpieczeństwo przed niedozwolonym lub niezgodnym z prawem Przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem i za pomocą odpowiednich środków technicznych i organizacyjnych.

2. Administrator przetwarza Dane Osobowe wyłącznie w przypadkach zakreślonych przepisami prawa.

3. Do przetwarzania Danych Osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie Administratora (czyli Użytkownicy), zgodnie z wzorem stanowiącym **Załącznik nr 3** do Polityki.

4. Rozwiązanie stosunku pracy lub innego stosunku prawnego, na podstawie którego Użytkownik uzyskał dostęp do Danych Osobowych, bądź zmiana zakresu obowiązków (powodująca, że dostęp Użytkownika do wszystkich lub niektórych Danych Osobowych nie jest już konieczny), skutkuje utratą dostępu do Danych Osobowych lub zmianą zakresu dostępu i podlega odnotowaniu w ewidencji osób upoważnionych do przetwarzania Danych Osobowych, której wzór stanowi **Załącznik nr 4** do Polityki.

5. Administrator zapoznaje osoby upoważnione do przetwarzania Danych Osobowych z przepisami o ochronie danych osobowych, w szczególności z przepisami RODO oraz niniejszej Polityki.

6. Jeżeli przetwarzanie ma być dokonywane w imieniu Administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi przepisane prawem i wymogi określone w Polityce oraz by chroniło prawa osób, których Dane Osobowe dotyczą. Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy według wzoru stanowiącego **Załącznik nr 9** do Polityki. Administrator prowadzi ewidencję zawartych umów o przetwarzanie Danych Osobowych zgodnie z wzorem stanowiącym **Załącznik nr 6** do Polityki.

§ 5
OBOWIĄZKI ADMINISTRATORA

1. Do zadań Administratora Danych Osobowych należy w szczególności:

   1.1. organizacja ochrony Danych Osobowych w Spółce, w tym podział zadań i obowiązków w zakresie ochrony Danych Osobowych;

   1.2. podejmowanie decyzji o celach i środkach przetwarzania oraz stosowanych technik zabezpieczenia Danych Osobowych;

   1.3. podejmowanie odpowiednich działań w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa Danych Osobowych;

   1.4. wydawanie, zmiana i cofanie upoważnień do przetwarzania Danych Osobowych dla wszystkich osób mających dostęp do Danych Osobowych przetwarzanych w Spółce;

   1.5. regularna ocena ryzyka oraz ocena skutków przetwarzania Danych Osobowych;

   1.6. zawieranie porozumień z podmiotami przetwarzającymi Dane Osobowe w imieniu Administratora oraz prowadzenie ewidencji umów zawartych z podmiotami przetwarzającymi zgodnie z wzorem stanowiącym **Załącznik nr 6** do Polityki;

   1.7. prowadzenie rejestru incydentów naruszenia bezpieczeństwa Przetwarzania Danych Osobowych według wzoru stanowiącego **Załącznik nr 5** do niniejszej Polityki;

   1.8. dokonywanie identyfikacji zasobów Danych Osobowych, zależności między zasobami, identyfikacji sposobów wykorzystania danych, w szczególności przetwarzania danych wrażliwych, przetwarzania danych niezidentyfikowanych, przetwarzania danych dzieci, profilowania;

   1.9. weryfikowanie, czy dochodzi do przypadków współadministrowania Danymi Osobowymi;

2. Administrator prowadzi ewidencję osób dopuszczonych do przetwarzania Danych Osobowych, której wzór stanowi **Załącznik nr 4** do niniejszej Polityki. W ewidencji tej odnotowuje się:

   2.1. imię i nazwisko osoby upoważnionej do przetwarzania Danych Osobowych;

   2.2. stanowisko i oznaczenie komórki organizacyjnej;

   2.3. datę udzielenia, zmiany zakresu i cofnięcia upoważnienia do Przetwarzania Danych Osobowych;

   2.4. oznaczenie Zbioru danych, do którego Użytkownik posiada dostęp.

3. Administrator prowadzi Rejestr czynności Przetwarzania Danych Osobowych, w którym odnotowuje się każdą czynność Przetwarzania Danych Osobowych, wskazując co najmniej:

   3.1. imię, nazwisko lub nazwę, dane kontaktowe Administratora oraz wszelkich współadministratorów, a gdy ma to zastosowanie również przedstawiciela Administratora;

   3.2. nazwę czynności przetwarzania;

3.3. cele przetwarzania;

3.4. opis kategorii osób, których Dane Osobowe dotyczą i kategorii Danych Osobowych;

3.5. kategorię odbiorców, którym Dane Osobowe zostały lub zostaną ujawnione;

3.6. przekazanie Danych Osobowych do państwa trzeciego lub organizacji międzynarodowej wraz z ich nazwą (o ile dotyczy);

3.7. planowane terminy usunięcia poszczególnych kategorii Danych Osobowych (o ile jest możliwe);

3.8. ogólny opis technicznych i organizacyjnych środków bezpieczeństwa;

3.9. podstawę Przetwarzania Danych Osobowych.

4. Administrator inwentaryzuje zgody na przetwarzanie Danych Osobowych oraz inwentaryzuje i przygotowuje uzasadnienie przypadków, gdy zgodnie z RODO dochodzi do Przetwarzania Danych Osobowych na podstawie innej niż zgoda.

5. Administrator przekazuje osobom, których Dane Osobowe przetwarza, wszelkie wymagane prawem informacje zarówno w czasie pozyskiwania Danych Osobowych, jak i po ich zebraniu, o ile przepisy prawa nakładają na Administratora dodatkowe obowiązki informacyjne oraz dokumentuje realizację obowiązków informacyjnych.

6. Administrator zapewnia, aby żądania osób, których Dane Osobowe dotyczą były realizowane w terminach wskazanych w RODO.

§ 6

ZADANIA ADMINISTRATORA SYSTEMU INFORMATYCZNEGO ORAZ OSÓB UPOWAŻNIONYCH

1. Do zadań Administratora Systemu Informatycznego należy:
   1.1. przeciwdziałanie dostępowi osób nieupoważnionych do Systemu informatycznego, w którym przetwarzane są Dane Osobowe, w szczególności poprzez prawidłową konfigurację systemów i urządzeń;

   1.2. przydzielenie każdemu Użytkownikowi identyfikatora i hasła oraz nadawanie, modyfikacja oraz ograniczane uprawnień Użytkowników zgodnie z decyzją Administratora;

   1.3. zapewnianie niezawodności działania serwerów, sieci lokalnej, komputerów i innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji;

   1.4. nadzorowanie działania mechanizmów uwierzytelniania Użytkowników oraz kontroli dostępu do systemów służących do Przetwarzania Danych Osobowych.

2. Do obowiązków wszystkich osób upoważnionych do Przetwarzania Danych Osobowych należy:

   2.1. przetwarzanie Danych Osobowych wyłącznie w zakresie i celu, jaki wynika z obowiązków służbowych oraz nadanego upoważnienia do Przetwarzania Danych Osobowych;

   2.2. zachowanie w poufności informacji, z jakimi zapoznały się w związku z pełnionymi obowiązkami służbowymi, w tym danych uwierzytelniających (np. haseł, loginów);

   2.3. dbałość o bezpieczeństwo nośników i urządzeń służących do Przetwarzania Danych Osobowych zarówno w siedzibie Spółki, i jak i poza nią;

   2.4. zgłaszanie wszystkich podejrzanych lub faktycznych nieprawidłowości w procesie Przetwarzania Danych Osobowych Administratorowi;

   2.5. postępowanie zgodnie z wewnętrznymi regulacjami dotyczącymi Przetwarzania Danych Osobowych, w szczególności dotyczących zabezpieczenia Danych Osobowych i nośników

Danych Osobowych, opisanych w Instrukcji zarządzania systemem informatycznym, której wzór stanowi **Załącznik nr 8** do Polityki.

§ 7
OBOWIĄZKI INFORMACYJNE

1. Jeżeli Dane Osobowe zbierane są od osoby, której dotyczą, Administrator informuje ją, zgodnie z wzorem stanowiącym **Załącznik nr 1** do Polityki, o:
   1.1. swojej tożsamości i danych kontaktowych;
   1.2. danych kontaktowych inspektora danych osobowych, jeśli istnieje;
   1.3. celu Przetwarzania Danych Osobowych oraz podstawie prawnej przetwarzania;
   1.4. Odbiorcach danych lub ich kategoriach, jeśli istnieją;
   1.5. zamiarze przekazania Danych Osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu przez Komisję Europejską lub braku stwierdzenia.
2. Przetwarzanie przez Administratora Danych Osobowych osoby, której Dane Osobowe dotyczą, wymaga dodatkowo wyrażenia przez tę osobę pisemnej zgody według wzoru stanowiącego **Załącznik nr 2** do Polityki.

§ 8
INCYDENTY DOTYCZĄCE NARUSZENIA OCHRONY DANYCH

1. Administrator stosuje procedury działania w przypadku naruszenia ochrony Danych Osobowych, pozwalające na identyfikację i weryfikację naruszenia, a w razie potrzeby również niezwłocznie informuje właściwy organ nadzorczy oraz zawiadamia osobę, której Dane Osobowe dotyczą.
2. W razie naruszenia Danych Osobowych lub zagrożenia naruszeniem Administrator podejmuje odpowiednie środki zaradcze.

§ 9

STOSOWANE ŚRODKI ORGANIZACYJNE

1. Administrator stosuje zabezpieczenia pomieszczeń, biur, miejsc i nośników danych, bez względu na ich formę, które chronią przetwarzane Dane Osobowe przed dostępem osób nieupoważnionych.
2. Do pomieszczeń, w których przetwarzane są Dane Osobowe, dostęp mają wyłącznie osoby upoważnione. Osoby nieuprawnione mogą przebywać w obszarze przetwarzania wyłącznie za zgodą Administratora lub w obecności osoby upoważnionej do Przetwarzania Danych Osobowych.
3. Administrator zapoznaje każdego Użytkownika o obowiązujących w Spółce zasadach ochrony Danych Osobowych, na dowód, czego Użytkownik składa oświadczenie, którego wzór stanowi **Załącznik nr 3a** do Polityki. Administrator prowadzi ewidencję osób, które zapoznały się z obowiązującymi w Spółce zasadami ochrony Danych Osobowych, zgodnie z wzorem stanowiącym **Załącznik nr 7** do Polityki.
4. Instrukcja zarządzania systemem informatycznym, zawierająca opis środków technicznych dotyczących zabezpieczenia Systemu informatycznego, stanowi **Załącznik nr 8** do Polityki.

§ 10
POSTANOWIENIA KOŃCOWE

1. Polityka dostępna jest w siedzibie Administratora.
2. Polityka wchodzi w życie z dniem 25 maja 2018 roku.
3. Załączniki do Polityki stanowią jej integralną część i są nimi:

3.1. Załącznik nr 1 – Wzór informacji o przetwarzaniu danych osobowych

3.2. Załącznik nr 2 – Wzór oświadczenia o wyrażeniu zgody na przetwarzanie Danych Osobowych

3.3. Załącznik nr 3 – Wzór upoważnienia do przetwarzania Danych Osobowych

3.4. Załącznik nr 3a – Oświadczenie osoby upoważnionej do przetwarzania Danych Osobowych

3.5. Załącznik nr 4 – Ewidencja osób upoważnionych do przetwarzania Danych Osobowych

3.6. Załącznik nr 5 – Ewidencja incydentów dotyczących przetwarzania Danych Osobowych

3.7. Załącznik nr 6 – Ewidencja umów o przetwarzanie Danych Osobowych

3.8. Załącznik nr 7 – Ewidencja osób, które zapoznały się z dokumentacją dotyczącą ochrony Danych Osobowych.

3.9. Załącznik nr 8 – Instrukcja zarządzania Systemem informatycznym

3.10. Załącznik nr 9 – Wzór umowy o powierzeniu do przetwarzania Danych Osobowych