

Spółdzielnia Budowlano-Mieszkaniowa „SKARBOWIEC”

ul. Grójecka 41, 02-031 Warszawa

zarzad@skarbowiec.waw.pl

UCHWAŁA NR 1/2021

Zarządu Spółdzielni Budowlano-Mieszkaniowej „SKARBOWIEC” w Warszawie
z dnia 5 stycznia 2021 roku w sprawie:
powołania pani Katarzyny Prokopowicz na stanowisko Inspektora Ochrony Danych
oraz przyjęcia Polityki Bezpieczeństwa Ochrony Danych Osobowych w SBM SKARBOWIEC

§ 1.

W związku z art. 37 ust. 4 RODO Zarząd Spółdzielni powołuje panią Katarzynę Prokopowicz na stanowisko Inspektora Ochrony Danych (IOD).

§ 2.

Powołana na stanowisko IOD pani Katarzyna Prokopowicz świadczy usługi dla Spółdzielni na podstawie odrębnej umowy cywilno-prawnej. Umowny zakres usług wypełnia w całości obowiązki podmiotu przetwarzającego dane zgodnie z par. 39 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO).

§ 3.

Zgodnie z wymogami określonymi w art. 37 ust. 7 RODO podstawowe informacje kontaktowe kierujące do IOD w zakresie imienia, nazwiska, numeru telefonu oraz adresu poczty elektronicznej zostaną ujawnione w serwisie internetowym Spółdzielni.

§ 4.

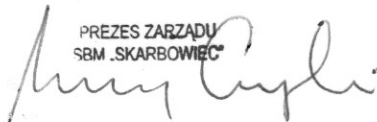
Zarząd przyjmuje jako obowiązującą Politykę Bezpieczeństwa Ochrony Danych Osobowych w SBM SKARBOWIEC oraz wzory powiązanych z nią dokumentów, które stanowią załącznik do niniejszej uchwały. Dokumenty stanowiące załącznik do uchwały podlegają publikacji na stronie internetowej Spółdzielni.

§ 5.

Uchwała wchodzi w życie z dniem podjęcia.

MACIEJ CZYŃSKI

PREZES ZARZĄDU
SBM „SKARBOWIEC”



Za uchwałą głosów: 2

Przeciw uchwale głosów: 0



ROBERT KRUPA

CZŁONEK ZARZĄDU
SBM „SKARBOWIEC”

SBM Skarbowiec	Nazwa dokumentu: Polityka Bezpieczeństwa Ochrony Danych Osobowych w SBM Skarbowiec			
	Edycja:	2.0	Obowiązuje od:	05.01.2021
	Uchwała nr	1/2021	Data uchwalenia:	05.01.2021
	Zastępuje:	Polityka ochrony danych osobowych		
<i>Własność SBM Skarbowiec. Do użytku wewnętrznego. Podlega nadzorowi.</i>				
Opracował		Zatwierdził		
Katarzyna Prokopowicz		Zarząd		

I. POSTANOWIENIA OGÓLNE

§ 1.

Przedmiot Polityki

1. Spółdzielnia Budowlano-Mieszkaniowa Skarbowiec (SBM Skarbowiec) z siedzibą w Warszawie (02-042) przy ul. Grójeckiej 41 jest Administratorem Danych Osobowych w rozumieniu art. 4 pkt 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE L z dnia 4 maja 2016 r.).
2. W celu zapewnienia przetwarzania danych osobowych przez Administratora Danych Osobowych zgodnie z obowiązującym prawem, a w szczególności zapewnienia najwyższej ochrony przetwarzanych danych osobowych, Administrator Danych Osobowych przyjmuje niniejszą Politykę.
3. Niniejsza Polityka jest zgodna z:
 - a) 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) (Dz. U. UE L z dnia 4 maja 2016 r. — dalej: RODO),
 - b) ustawą o ochronie danych osobowych z dn. 10 maja 2018 r. (Dz. U. 2018 poz. 1000),
 - c) ustawą z dnia 15 grudnia 2000 r. o spółdzielniach mieszkaniowych,
 - d) ustawą z dnia 16 września 1982 r. Prawo spółdzielcze,
 - e) innymi obowiązującymi przepisami krajowymi i międzynarodowymi,

K. C.

U. R.

- f) statutem SBM Skarbowiec.
4. Polityka stanowi część składową systemu ochrony danych osobowych obowiązującego u Administratora Danych Osobowych, określając w szczególności:
- zasady przetwarzania danych osobowych u Administratora Danych Osobowych;
 - zasady zapewniania ochrony przetwarzanych danych osobowych;
 - procedury stosowane u Administratora Danych Osobowych;
 - wzorce dokumentów i formularzy stosowanych przez Administratora Danych Osobowych;
5. Niniejsza Polityka jest środkiem prawnym przewidzianym w art. 24 ust. 2 RODO.

§ 2.

Definicje

Na potrzeby niniejszej Polityki przyjmuje się następujące definicje użytych pojęć:

	Pojęcie	Definicja
a)	Administrator Danych Osobowych	Spółdzielnia Budowlano-Mieszkaniowa Skarbowiec (SBM Skarbowiec), ul. Grójecka 41, 02-031 NIP: 5250007046 KRS: 0000410983 REGON: 000490547
b)	Administrator Systemów Informatycznych	osoba wyznaczona przez Administratora Danych Osobowych, odpowiedzialna za funkcjonowanie i bezpieczeństwo systemów informatycznych; jeżeli taka osoba nie została wyznaczona, Administrator Danych Osobowych samodzielnie zarządza systemami informatycznymi.
c)	Dane osobowe	wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej
d)	Dane dzieci	dane osobowe osób fizycznych poniżej 16. roku życia
e)	Dane karne	dane osobowe dotyczące wyroków skazujących i czynów zabronionych lub powiązanych środków bezpieczeństwa
f)	Dane szczególnych kategorii	dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych; dane genetyczne; dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej; dane dotyczące zdrowia, seksualności lub orientacji seksualnej osoby fizycznej
g)	Dane zwykłe	dane osobowe, które nie są danymi szczególnych kategorii

U. An

2
U. Płog.

h)	Dostępność	zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy, kiedy jest to potrzebne
i)	Incydent	zdarzenie mogące wpłynąć na bezpieczeństwo danych osobowych w zakresie dostępności, integralności, poufności lub odporności systemów i usług przetwarzania. Incydent może prowadzić do naruszenia ochrony danych osobowych, ale nie musi
j)	Integralność	zapewnienie dokładności i kompletności informacji oraz metod przetwarzania
k)	Naruszenie ochrony danych osobowych	naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych
l)	Odbiorca danych osobowych	osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną (osobą) trzecią. Nie uznaje się za odbiorców organów publicznych, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii Europejskiej lub prawem państwa członkowskiego
m)	Odporność	zdolność systemów informatycznych do prawidłowego funkcjonowania mimo dużego obciążenia
n)	Osoba upoważniona	osoba upoważniona przez Administratora Danych Osobowych do przetwarzania danych osobowych w określonym przez niego zakresie
o)	Państwo trzecie	państwo nienależące do Unii Europejskiej oraz Europejskiego Obszaru Gospodarczego
p)	Podmiot danych	osoba fizyczna, której dane osobowe dotyczą
q)	Podmiot przetwarzający	osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora Danych Osobowych
r)	Polityka	niniejsza „Polityka bezpieczeństwa ochrony danych osobowych w SBM Skarbowiec”
s)	Poufność	zapewnienie, że dane osobowe są dostępne jedynie dla osób upoważnionych
t)	Profilowanie	dowolna forma zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się
u)	Przetwarzanie danych osobowych	operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przestanie,

u am

		rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie
v)	Pseudonimizacja	przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej
w)	Rozliczalność	wykazanie przez Administratora Danych Osobowych, że przestrzega przepisów dotyczących ochrony danych osobowych w prowadzonych procesach przetwarzania danych osobowych
x)	Strona (osoba) trzecia	osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż: – osoba, której dane dotyczą, – Administrator Danych Osobowych i współadministrator danych osobowych, – podmiot przetwarzający, – osoba upoważniona.
y)	System informatyczny	zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych
z)	System ochrony danych osobowych	całokształt środków technicznych, organizacyjnych i prawnych wraz z niezbędną dokumentacją, wdrożonych przez Administratora Danych Osobowych, służących zapewnieniu, że przetwarzanie danych osobowych będzie odbywało się zgodnie z przepisami z zakresu ochrony danych osobowych
aa)	Współadministrator danych osobowych	osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który wspólnie z Administratorem Danych Osobowych decyduje o celach i sposobach przetwarzania danych osobowych
bb)	Zagrożenie	potencjalna możliwość wystąpienia incydentu
cc)	Zbiór danych osobowych	uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie
dd)	Zgoda	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

u An

U. Rhy.

II. FUNDAMENTY I ZASADY OCHRONY DANYCH OSOBOWYCH

§ 3.

Fundamenty systemu ochrony danych osobowych

Administrator Danych Osobowych tworzy system ochrony danych osobowych w swojej organizacji, budując go na następujących fundamentach:

- a) **podejście oparte na ryzyku** — Administrator Danych Osobowych jest zobowiązany zidentyfikować ryzyka towarzyszące przetwarzaniu danych osobowych oraz ustalić ich wpływ na operacje związane z danymi osobowymi, a w szczególności na prawa i wolności osób fizycznych,
- b) **poszanowanie praw osób fizycznych** — Administrator Danych Osobowych, jak również wszystkie osoby zaangażowane w procesy przetwarzania danych osobowych, są zobowiązani ułatwić osobom fizycznym realizację ich praw związanych z ochroną danych osobowych,
- c) **legalność** — Administrator Danych Osobowych, jak również wszystkie osoby zaangażowane w procesy przetwarzania danych osobowych, są zobowiązani przeprowadzać jakiegokolwiek operacje związane z danymi osobowymi przy zachowaniu pełnej zgodności z obowiązującym prawem,
- d) **bezpieczeństwo** — Administrator Danych Osobowych jest zobowiązany zapewnić bezpieczeństwo przetwarzania danych osobowych, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze,
- e) **rozliczalność** — Administrator Danych Osobowych, jak również wszystkie osoby zaangażowane w procesy przetwarzania danych osobowych, są zobowiązani dokumentować sposób spełnienia obowiązków wynikających z przepisów z zakresu ochrony danych osobowych.

§ 4.

Zasady ochrony danych osobowych

Administrator Danych Osobowych przetwarza dane osobowe w oparciu o następujące zasady:

- a) **zasada zgodności z prawem, rzetelności i przejrzystości** — dane osobowe są przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą,
- b) **zasada ograniczenia celu** — dane osobowe są zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami,
- c) **zasada minimalizacji danych** — dane osobowe są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane,

h. Am

U. Rhyg.

- d) **zasada prawidłowości** — dane osobowe są 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,
- e) **zasada czasowości** — dane osobowe są 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,
- f) **zasada integralności i poufności** — dane osobowe są 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.

III. PODMIOTY TWORZĄCE SYSTEM OCHRONY DANYCH OSOBOWYCH

§ 5.

Współadministrator danych osobowych

1. Administrator Danych Osobowych może wspólnie ustalać cele i sposoby przetwarzania danych osobowych ze współadministratorem danych osobowych — jeżeli taka konieczność wynika z przedsięwzięć realizowanych przez Administratora Danych Osobowych.
2. Administrator Danych Osobowych jest zobowiązany zawrzeć ze współadministratorem danych osobowych umowę o współadministrowanie danymi osobowymi.
3. W umowie o współadministrowanie danymi osobowymi należy określić w szczególności:
 - a) zakresy odpowiedzialności Administratora Danych Osobowych i współadministratora danych osobowych;
 - b) sposób realizowania obowiązków wynikających z przepisów z zakresu ochrony danych osobowych;
 - c) sposób spełnienia obowiązków informacyjnych z art. 13 RODO i art. 14 RODO;
 - d) punkt kontaktowy — jeżeli jest to wskazane;
 - e) relacje pomiędzy Administratorem Danych Osobowych i współadministratorem danych osobowych a podmiotami danych;
 - f) sposób przekazania podmiotom danych treści uzgodnień pomiędzy Administratorem Danych Osobowych a współadministratorem danych osobowych.

§ 6.

Inspektor Ochrony Danych

1. W przypadkach wskazanych w art. 37 ust. 1 RODO lub w prawie polskim Administrator Danych Osobowych jest zobowiązany wyznaczyć Inspektora Ochrony Danych.

U. An

⁶ *U. Rlyg.*

2. W przypadkach innych niż wskazane w ust. 1, Administrator Danych Osobowych może podjąć decyzję o dobrowolnym powołaniu Inspektora Ochrony Danych.
3. Administrator Danych Osobowych zawiadamia Prezesa Urzędu Ochrony Danych Osobowych w terminie 14 dni o:
 - a) wyznaczeniu Inspektora Ochrony Danych, podając jego dane kontaktowe;
 - b) zmianie Inspektora Ochrony Danych, podając jego dane kontaktowe;
 - c) rezygnacji z wyznaczania Inspektora Ochrony Danych, jeżeli wcześniej był wyznaczony.
4. Administrator Danych Osobowych może zatrudnić Inspektora Ochrony Danych na podstawie umowy o pracę lub na podstawie cywilnoprawnej umowy o świadczenie usług.
5. Z uwagi na konflikt interesów Inspektorem Ochrony Danych nie może być osoba zatrudniona na stanowisku, które decyduje o celach przetwarzania danych osobowych.
6. Inspektor Ochrony Danych ma za zadanie:
 - a) informować Administratora Danych Osobowych oraz osoby przez niego zatrudnione, które przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy prawa;
 - b) doradzać w sprawie przestrzegania przepisów z zakresu ochrony danych osobowych;
 - c) monitorować przestrzeganie przepisów z zakresu ochrony danych osobowych, niniejszej Polityki oraz innych dokumentów Administratora Danych Osobowych;
 - d) monitorować podział obowiązków;
 - e) podejmować działania zwiększające świadomość w zakresie ochrony danych osobowych;
 - f) przeprowadzać szkolenia osób zatrudnionych w zakresie ochrony danych osobowych;
 - g) prowadzić audyty;
 - h) udzielać na żądanie Administratora Danych Osobowych zaleceń co do oceny skutków dla ochrony danych osobowych oraz monitorować jej wykonanie zgodnie z art. 35 RODO;
 - i) współpracować z Prezesem Urzędu Ochrony Danych Osobowych;
 - j) pełnić funkcję punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzić konsultacje we wszelkich innych sprawach.
7. Administrator Danych Osobowych jest zobowiązany zapewnić, by Inspektor Ochrony Danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.
8. Administrator Danych Osobowych jest zobowiązany wspierać Inspektora Ochrony Danych w wypełnianiu przez niego zadań, o których mowa w ust. 7, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.

U. C...

7 *U. R...*

9. Administrator Danych Osobowych zapewnia, że:
 - a) Inspektor Ochrony Danych nie otrzymuje instrukcji dotyczących wykonywania zadań;
 - b) nie karze Inspektora Ochrony Danych za wypełnianie swoich zadań;
 - c) nie odwołuje Inspektora Ochrony Danych za wykonywanie przez niego obowiązków.
10. Inspektor Ochrony Danych podlega bezpośrednio Administratorowi Danych Osobowych lub najwyższemu kierownictwu Administratorów Danych Osobowych.

§ 7.

Osoby upoważnione

1. Przetwarzania danych osobowych w ramach struktury Administratora Danych Osobowych mogą dokonywać wyłącznie osoby upoważnione przez Administratora Danych Osobowych.
2. Administrator Danych Osobowych zapewnia, aby żadna z osób upoważnionych nie miała dostępu do większej ilości danych osobowych i procesów przetwarzania danych osobowych niż jest to konieczne do prawidłowego wypełniania obowiązków i zadań.
3. Procedura nadawania i odbierania upoważnień stanowi Załącznik 12.
4. Osoba upoważniona do przetwarzania danych osobowych przed przystąpieniem do czynności ma obowiązek:
 - a) zapoznać się z dokumentami z zakresu ochrony danych osobowych w zakresie ustalonym przez Administratora Danych Osobowych i/lub odbyć szkolenie z zakresu ochrony danych osobowych,
 - b) złożyć oświadczenie na piśmie o zapoznaniu się z dokumentami z zakresu ochrony danych osobowych i/lub o ewentualnym odbyciu szkolenia z zakresu ochrony danych osobowych.
5. Wzory oświadczeń, o których mowa w ust. 4, stanowią Zał. 1-3 do procedury nadawania i odbierania upoważnień zgodnie z Załącznik 12.
6. Oświadczenia, o których mowa w ust. 4, są dołączane do umowy zawartej z osobą upoważnioną lub do akt osobowych osoby upoważnionej.
7. Administrator Danych Osobowych zapewnia osobom upoważnionym dostęp do dokumentów z zakresu ochrony danych, z wyjątkiem tych dokumentów, które nie powinny być dostępne dla wszystkich osób upoważnionych.
8. Obowiązki określone w ust. 4 nie dotyczą osób, które są dopuszczane do przetwarzania danych osobowych incydentalnie (np. w celu naprawy sprzętu). W takiej sytuacji należy wskazać w treści zawartej umowy obowiązek przestrzegania ochrony danych osobowych oraz przekazać najważniejsze informacje na temat ochrony danych osobowych. W zależności od sytuacji z takimi osobami można zawrzeć również umowę powierzenia.
9. Inspektor Ochrony Danych prowadzi w imieniu Administratora Danych Osobowych ewidencję osób upoważnionych do przetwarzania danych osobowych.

§ 8.

U. An

⁸
U. Rhyf

Podmioty przetwarzające

1. Administrator Danych Osobowych może powierzyć przetwarzanie danych osobowych podmiotowi przetwarzającemu w zależności od własnych potrzeb.
2. Administrator Danych Osobowych jest obowiązany powierzać przetwarzanie danych osobowych tylko takim podmiotom przetwarzającym, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. Zakazane jest korzystanie z usług podmiotów przetwarzających, które takich gwarancji nie dają.
3. Wzór umowy powierzenia przetwarzania danych osobowych stanowi Załącznik nr 4.
4. W przypadku korzystania przez podmiot przetwarzający z usług innego podmiotu przetwarzającego, który nie daje analogicznych gwarancji, o jakich mowa w ust. 2, Administrator Danych Osobowych jest obowiązany wnieść sprzeciw, a w innych przypadkach — może wnieść sprzeciw, jeżeli istnieją ku niemu podstawy.
5. Inspektor Ochrony Danych jest obowiązany w imieniu Administratora Danych Osobowych kontrolować przestrzeganie przez podmiot przetwarzający przepisów RODO przez cały okres trwania umowy.
6. W przypadku naruszenia przez podmiot przetwarzający przepisów RODO Administrator Danych Osobowych jest obowiązany niezwłocznie zaprzestać współpracy z podmiotem przetwarzającym.
7. Administrator Danych Osobowych prowadzi ewidencję podmiotów przetwarzających, z którymi zawarł umowy o powierzenie przetwarzania danych osobowych.
8. Wzór ewidencji podmiotów przetwarzających stanowi Załącznik 5.

§ 9.

Administrator Danych Osobowych jako podmiot przetwarzający

1. W związku z prowadzoną działalnością Administrator Danych Osobowych może być podmiotem przetwarzającym dla innego administratora danych osobowych.
2. W przypadkach wskazanych w ust. 1 Administrator Danych Osobowych zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.
3. W przypadkach wskazanych w ust. 1 Administrator Danych Osobowych wywiązuje się z obowiązków przewidzianych w umowie powierzenia przetwarzania danych osobowych, którą zawiera z innym administratorem danych osobowych.
4. W przypadkach wskazanych w ust. 1 Administrator Danych Osobowych może być zobowiązany do wyznaczenia Inspektora Ochrony Danych w związku z umową o powierzeniu przetwarzania danych osobowych zawartą z innym administratorem danych osobowych. W takiej sytuacji § 6 stosuje się odpowiednio.
5. W przypadkach wskazanych w ust. 1 Administrator Danych Osobowych prowadzi rejestr wszystkich kategorii czynności przetwarzania.

U. Am

⁹ *U. Rhyf.*

6. Wzór rejestru wszystkich kategorii czynności przetwarzania stanowi Załącznik 6.

§ 10.

Odbiorcy danych osobowych

1. Administrator Danych Osobowych ujawnia dane osobowe odbiorcom danych osobowych wyłącznie po zweryfikowaniu podstawy prawnej takiego ujawnienia.
2. W przypadku braku podstawy prawnej, o której mowa w ust. 1, Administrator Danych Osobowych odmawia ujawnienia danych osobowych jakimukolwiek odbiorcy danych osobowych.
3. Administrator Danych Osobowych prowadzi ewidencję odbiorców danych osobowych.
4. Wzór ewidencji odbiorców danych osobowych stanowi Załącznik 7.

IV. PRZETWARZANIE DANYCH OSOBOWYCH

§ 11.

Zarządzanie ryzykiem

1. Administrator Danych Osobowych wdraża i utrzymuje procedurę zarządzania ryzykiem.
2. Administrator Danych Osobowych jest zobowiązany uwzględniać ryzyko w planowanych i prowadzonych procesach przetwarzania danych osobowych.
3. Procedura zarządzania ryzykiem stanowi Załącznik 11.

§ 12.

Ocena skutków dla ochrony danych osobowych

1. W przypadkach wskazanych w art. 35 ust. 1 RODO, art. 35 ust. 3 RODO oraz w odniesieniu do operacji przetwarzania znajdujących się w wykazie publikowanym przez Prezesa Urzędu Ochrony Danych Osobowych na podstawie art. 35 ust. 4 RODO Administrator Danych Osobowych jest zobowiązany przeprowadzić ocenę skutków dla ochrony danych osobowych.
2. Ocena skutków dla ochrony danych osobowych nie jest wymagana w odniesieniu do operacji przetwarzania znajdujących się w wykazie publikowanym przez Prezesa Urzędu Ochrony Danych Osobowych na podstawie art. 35 ust. 5 RODO.

§ 13.

Uprzednie konsultacje z Prezesem Urzędu Ochrony Danych Osobowych

1. Jeżeli z oceny skutków dla ochrony danych osobowych wynika, że przetwarzanie powodowałoby wysokie ryzyko, gdyby Administrator Danych Osobowych nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania Administrator Danych Osobowych jest zobowiązany skonsultować się z Prezesem Urzędu Ochrony Danych Osobowych.

U. An

U. Rlyp.

§ 14.

Ochrona danych w fazie projektowania I domyślna ochrona danych

1. Administrator Danych Osobowych jest obowiązany uwzględniać ochronę danych osobowych w fazie projektowania nowych systemów, programów, aplikacji, usług, a także w fazie projektowania nowych procesów i sposobów przetwarzania danych osobowych (privacy by design).
2. Administrator Danych Osobowych jest obowiązany zapewnić domyślną ochronę danych osobowych, tj. domyślnie mogą być przetwarzane tylko te dane osobowe, które są niezbędne do osiągnięcia konkretnego celu przetwarzania (privacy by default). Rezygnacja z prywatności lub jej ograniczenie mogą nastąpić tylko na wyraźne żądanie podmiotu danych.

§ 15.

Inwentaryzacja

1. Administrator Danych Osobowych szczegółowo inwentaryzuje posiadane dane osobowe oraz procesy z nimi związane, ze szczególnym uwzględnieniem:
 - a) danych szczególnych,
 - b) danych karnych,
 - c) danych dzieci,
 - d) danych osobowych poddanych profilowaniu i zautomatyzowanemu podejmowaniu decyzji.
2. W celu zapewnienia pełnej kontroli nad przetwarzaniem danych osobowych oraz zapewnienia bezpieczeństwa przetwarzania danych osobowych Administrator Danych Osobowych prowadzi ewidencję obszarów, w których przetwarzane są dane — wzór ewidencji obszarów stanowi Załącznik 8,
3. Administrator Danych Osobowych kontroluje przetwarzanie danych niezidentyfikowanych, o których mowa w art. 11 ust. 1 RODO, w szczególności w odniesieniu do nagrań (wizualnych, dźwiękowych, audiowizualnych), korespondencji elektronicznej i wszelkich innych strumieni, które potencjalnie mogą zawierać dane osobowe.

§ 16.

Rejestr czynności przetwarzania danych osobowych

1. Administrator Danych Osobowych prowadzi i aktualizuje rejestr czynności przetwarzania danych osobowych, który jest najważniejszym dokumentem w zakresie ochrony danych osobowych.
2. Rejestr czynności przetwarzania danych osobowych służy:
 - a) inwentaryzowaniu i monitorowaniu sposobu przetwarzania danych osobowych;

U. Cur

11 *U. Płuc*

- b) dokumentowaniu czynności przetwarzania danych osobowych;
 - c) wykazaniu realizacji zasady rozliczalności.
3. Wzór rejestru czynności przetwarzania danych osobowych stanowi Załącznik 9.

§ 17.

Identyfikacja i weryfikacja podstaw prawnych przetwarzania danych osobowych

1. Administrator Danych Osobowych jest obowiązany przetwarzać dane osobowe wyłącznie w oparciu o konkretną podstawę prawną.
2. Administrator Danych Osobowych jest obowiązany w odniesieniu do każdej czynności przetwarzania danych osobowych zidentyfikować i zweryfikować podstawę prawną przetwarzania danych osobowych.
3. Administrator Danych Osobowych jest obowiązany monitorować zmiany legislacyjne i w miarę konieczności aktualizować dokumentację.
4. Administrator Danych Osobowych jest obowiązany wskazać w rejestrze o którym mowa w § 16 ust 3 podstawy przetwarzania.
5. Osoby upoważnione do przetwarzania danych osobowych mają obowiązek znać podstawy prawne, w oparciu o które wykonują czynności związane z danymi osobowymi.

§ 18.

Przetwarzanie danych osobowych na podstawie zgody

1. Administrator Danych Osobowych przetwarza dane osobowe na podstawie zgody tylko wówczas, gdy nie ma innej podstawy przetwarzania danych osobowych. Nie należy uzyskiwać zgody na przetwarzanie danych osobowych związanych z zawarciem i wykonaniem umowy lub w odniesieniu do takich danych osobowych, których obowiązek przetwarzania wynika z przepisów prawa.
2. Przed podjęciem decyzji o przetwarzaniu danych osobowych na podstawie zgody Administrator Danych Osobowych jest zobowiązany zweryfikować, czy dane osobowe są adekwatne do założonego celu przetwarzania.
3. Zabronione jest wywieranie przymusu w celu uzyskania zgody, w szczególności poprzez odmowę wykonania umowy w przypadku niewyrażenia zgody na przetwarzanie danych osobowych.
4. Zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie je odróżnić od pozostałych kwestii.
5. Zgody muszą być formułowane w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.
6. Zgoda może być cofnięta w każdym momencie. Administrator Danych Osobowych zapewnia, aby wycofanie zgody było równie proste, jak jej złożenie.
7. Administrator Danych Osobowych jest zobowiązany zapewnić system zarządzania zgodami, który pozwoli zweryfikować, czy dana osoba udzieliła zgody na przetwarzanie danych osobowych, czy i kiedy ją wycofała.

K. An

§ 19.

Profilowanie i zautomatyzowane podejmowanie decyzji

1. Jeżeli Administrator Danych Osobowych podejmuje czynności profilowania lub zautomatyzowanego podejmowania decyzji, jest zobowiązany zapewnić, aby te czynności odbywały się zgodnie z prawem.

§ 20.

Minimalizacja

1. Administrator Danych Osobowych jest zobowiązany przestrzegać zasady minimalizacji.
2. W celu zapewnienia realizacji zasady minimalizacji Administrator Danych Osobowych w szczególności:
 - a) weryfikuje ilość przetwarzanych danych osobowych — Administrator Danych Osobowych nie może przetwarzać większej ilości danych osobowych niż to wynika z założonego celu;
 - b) weryfikuje zakres przetwarzanych danych osobowych — Administrator Danych Osobowych nie może podejmować większej liczby czynności przetwarzania niż to wynika z założonego celu;
 - c) ogranicza dostęp do danych osobowych poprzez stosowanie środków prawnych (umowy z klauzulami poufności, system upoważnień), środków fizycznych (kontrola dostępu osób do budynków, pomieszczeń i systemów) oraz środków logicznych (kontrola uprawnień w systemach informatycznych i dostępu do systemów informatycznych);
 - d) ogranicza czas przetwarzania danych osobowych — Administrator Danych Osobowych nie może przetwarzać danych osobowych dłużej niż to wynika z założonego celu.
3. Procedura usuwania i niszczenia danych osobowych stanowi Załącznik 23.

§ 21.

Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych

1. Administrator Danych Osobowych jest obowiązany kontrolować, czy przekazuje jakiegokolwiek dane osobowe do państw trzecich lub organizacji międzynarodowych, w szczególności w przypadku korzystania z usług innych podmiotów.
2. Administrator Danych Osobowych jest obowiązany zidentyfikować i zweryfikować podstawę prawną przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych.
3. Administrator Danych Osobowych jest obowiązany monitorować zmiany legislacyjne i w miarę konieczności aktualizować dokumentację.

U. Ryp.

U. Ryp.

4. Przypadki przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych są odnotowywane w rejestrze czynności przetwarzania danych osobowych.

V. UPRAWNIENIA OSÓB FIZYCZNYCH

§ 22.

Obowiązki informacyjne

1. Administrator Danych Osobowych jest zobowiązany realizować obowiązki informacyjne, o których mowa w art. 13 RODO i art. 14 RODO.
2. Administrator Danych Osobowych spełnia obowiązek informacyjny:
 - a) w przypadku pozyskania danych bezpośrednio od podmiotu danych — w chwili pozyskiwania tych danych,
 - b) w przypadku pozyskiwania danych osobowych nie od podmiotu danych:
 - w rozsądnym terminie po pozyskaniu danych, jednak nie później niż w terminie miesiąca,
 - najpóźniej przy pierwszej komunikacji z podmiotem danych, jeżeli dane osobowe mają być wykorzystywane do komunikacji,
 - przy pierwszym ujawnieniu, jeżeli dane osobowe mają być ujawnione innemu odbiorcy.
3. Administrator Danych Osobowych nie jest zobowiązany zrealizować obowiązku informacyjnego w przypadku pozyskiwania danych od podmiotu danych, gdy podmiot danych już posiada te informacje.
4. Administrator Danych Osobowych nie jest zobowiązany zrealizować obowiązku informacyjnego w przypadku pozyskiwania danych nie od podmiotu danych, gdy:
 - a) podmiot danych dysponuje już tymi informacjami,
 - b) udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku, w szczególności w przypadku przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem warunków i zabezpieczeń, o których mowa w art. 89 ust. 1 RODO, lub o ile wykonanie obowiązku informacyjnego może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania. W takich przypadkach Administrator Danych Osobowych podejmuje odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy podmiotu danych, w tym udostępnia informacje publicznie,
 - c) pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii Europejskiej lub prawem polskim, lub

U. C.

- d) dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii Europejskiej lub w prawie polskim, w tym ustawowym obowiązkiem zachowania tajemnicy.
5. Administrator Danych Osobowych informuje podmiot danych o planowanej zmianie celu przetwarzania danych osobowych.
 6. Administrator Danych Osobowych informuje podmiot danych o planowanym uchyleniu ograniczenia przetwarzania danych osobowych.
 7. Administrator Danych Osobowych udziela informacji w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.
 8. Administrator Danych Osobowych jest zobowiązany opracować zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.

§ 23.

Rodzaje uprawnień osób fizycznych

1. Oprócz prawa do informacji, o których mowa w §22, każdemu podmiotowi danych przysługuje prawo do:
 - a) dostępu do danych osobowych i informacji o nich,
 - b) uzyskania kopii jego danych osobowych,
 - c) sprostowania danych osobowych i uzupełnienia niekompletnych danych osobowych;
 - d) usunięcia danych osobowych (prawo do bycia zapomnianym),
 - e) ograniczenia przetwarzania danych osobowych,
 - f) uzyskania informacji o odbiorcach danych osobowych w przypadku sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych,
 - g) uzyskania danych osobowych w określonym formacie i przesłania ich innemu administratorowi danych osobowych,
 - h) żądania przesłania danych osobowych innemu administratorowi danych osobowych przez Administratora Danych Osobowych,
 - i) wyrażenia sprzeciwu wobec przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. e RODO i art. 6 ust. 1 lit. f RODO, w tym profilowania,
 - j) wyrażenia sprzeciwu wobec marketingu bezpośredniego, w tym profilowania,
 - k) niepodlegania decyzji, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu.

§ 24.

Realizacja uprawnień osób fizycznych

1. Administrator Danych Osobowych jest zobowiązany ułatwiać podmiotom danych realizację ich uprawnień, o których mowa w § 23.
2. Administrator Danych Osobowych jest zobowiązany prowadzić komunikację z podmiotem danych w sprawie realizacji uprawnień związanych z przetwarzaniem danych osobowych.

U. Rhyg.

15 *U. Rhyg.*

3. Procesy realizacji praw osób fizycznych, których dane dotyczą są regulowane oddzielnymi procedurami stanowiącymi Załączniki 13-20 do niniejszej Polityki.

§ 25.

Pobieranie opłat za wykonywanie uprawnień

1. Udzielanie informacji, prowadzenie komunikacji oraz realizacja uprawnień związanych z przetwarzaniem danych osobowych co do zasady jest bezpłatne.
2. W przypadku, gdy żądania podmiotu danych są nieuzasadnione lub nadmierne, Administrator Danych Osobowych:
 - a) za prowadzenie komunikacji lub podjęcie żądanych działań może pobrać rozsądną opłatę, wynikającą z kosztów administracyjnych, albo
 - b) odmówić podjęcia działań w związku z żądaniem.
3. Pierwsza kopia danych osobowych przekazywana podmiotowi danych jest bezpłatna. Za wszelkie kolejne kopie Administrator Danych Osobowych może żądać rozsądnej opłaty, wynikającej z kosztów administracyjnych.

VI. BEZPIECZEŃSTWO PRZETWARZANIA DANYCH OSOBOWYCH

§ 26.

Obowiązek zapewnienia bezpieczeństwa przetwarzania danych osobowych

1. Administrator Danych Osobowych wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku przetwarzania danych osobowych.
2. Dobór odpowiednich środków technicznych i organizacyjnych następuje w ramach procedury zarządzania ryzykiem oraz ewentualnie w oparciu o ocenę skutków dla ochrony danych osobowych.
3. Dobór odpowiednich środków technicznych i organizacyjnych następuje z uwzględnieniem:
 - a) stanu wiedzy technicznej;
 - b) kosztów wdrażania;
 - c) charakteru, zakresu, kontekstu i celów przetwarzania;
 - d) ryzyka naruszenia praw i wolności osób fizycznych.

§ 27.

Systemy informatyczne

1. Administrator Danych Osobowych — jeżeli zajdzie taka potrzeba — może wyznaczyć Administratora Systemów Informatycznych. Jeżeli takiej osoby nie wyznacza, Administrator Danych Osobowych samodzielnie zarządza systemami informatycznymi.



2. Zasady związane z obsługą systemów informatycznych oraz ich zabezpieczeniem określa Instrukcja zarządzania systemami informatycznymi wraz z załącznikami.
3. Instrukcja, o której mowa w ust. 3, nie jest udostępniana ogółowi osób upoważnionych.

§ 28.

Zasady bezpieczeństwa i ich przestrzeganie

1. Administrator Danych Osobowych ustala i zapewnia przestrzeganie zasad bezpieczeństwa przez zatrudnionych.
2. Zasady bezpieczeństwa obowiązują wszystkie osoby przez niego zatrudnione, w tym praktykantów, stażystów i wolontariuszy, niezależnie od tego, czy biorą udział w przetwarzaniu danych osobowych i czy są upoważnione do przetwarzania danych osobowych.

§ 29.

Wykrywanie i klasyfikowanie incydentów z zakresu ochrony danych osobowych

1. Administrator Danych Osobowych jest zobowiązany wdrożyć środki umożliwiające jak najszybsze wykrywanie i klasyfikowanie incydentów związanych z ochroną danych osobowych oraz reagowanie na dostrzeżone incydenty.
2. Procedura postępowania w przypadku incydentów z zakresu ochrony danych osobowych stanowi Załączniki 21-22
3. Po stwierdzeniu naruszenia ochrony danych osobowych Administrator Danych Osobowych podejmuje wszelkie działania mające na celu zminimalizowanie skutków naruszenia, ustalenie przyczyn i okoliczności naruszenia, jak również wprowadza środki techniczne lub organizacyjne, mające zapobiegać występowaniu podobnych naruszeń w przyszłości.
4. Administrator Danych Osobowych dokumentuje wszystkie przypadki naruszeń w rejestrze naruszeń ochrony danych osobowych.

§ 30.

Zawiadamianie o naruszeniu ochrony danych osobowych

1. W przypadku naruszenia ochrony danych osobowych Administrator Danych Osobowych zawiadamia o tym naruszeniu:
 - a) Prezesa Urzędu Ochrony Danych Osobowych oraz
 - b) podmioty danych osobowych, których dane dotyczą,chyba, że zachodzi okoliczność wyłączająca obowiązek zawiadomienia.

A. Am

17 *A. Rępa*

VII. KONTROLA I DOSKONALENIE SYSTEMU OCHRONY DANYCH OSOBOWYCH

§ 31.

Audyt wewnętrzny

1. Przynajmniej raz na rok Inspektor Ochrony Danych przeprowadza kompleksowy audyt wewnętrzny w zakresie przestrzegania ochrony danych osobowych.
2. Audyt wewnętrzny może być dzielony na mniejsze zadania audytowe.
3. W przypadku naruszenia ochrony danych osobowych audyt wewnętrzny jest przeprowadzany niezwłocznie po usunięciu skutków naruszenia.

§ 32.

Kontrola przetwarzania danych osobowych

1. Przynajmniej raz na rok Administrator Danych Osobowych dokonuje przeglądu:
 - a) ilości przetwarzanych danych osobowych;
 - b) procesów przetwarzania danych osobowych;
 - c) upoważnień do przetwarzania danych osobowych;
 - d) użytkowników w systemach informatycznych.
2. W zakresie wynikającym z przeglądu, o którym mowa w ust. 1, dokonuje się niezbędnych usunięć i aktualizacji, aby zapewnić zgodność z niniejszą Polityką.

§ 33.

Przegląd Polityki i załączników

1. Przynajmniej raz na rok Administrator Danych Osobowych dokonuje przeglądu niniejszej Polityki oraz załączników.
2. Niniejsza Polityka wraz z załącznikami jest aktualizowana, rozwijana i modyfikowana:
 - a) na potrzeby dostosowania do zmiany stanu prawnego;
 - b) na potrzeby zwiększenia jej skuteczności;
 - c) w związku z potrzebami Administratora Danych Osobowych.

§ 34.

Szkolenia

1. Administrator Danych Osobowych jest zobowiązany podejmować działania na rzecz zwiększenia świadomości z zakresu ochrony danych osobowych wśród osób przez siebie zatrudnionych oraz podnoszenia ich wiedzy i kwalifikacji w tym zakresie.
2. Administrator Danych Osobowych zapewnia osobom przez siebie zatrudnionym szkolenia z zakresu ochrony danych osobowych, których częstotliwość oraz stopień zaawansowania zależy od pozycji zatrudnionego w systemie ochrony danych osobowych.

u Cu

VIII. WYKAZ ZAŁĄCZNIKÓW

§ 35.

Wykaz załączników

1. Poniższe Załączniki stanowią integralną część niniejszej Polityki:

Załącznik 1. Wzór oświadczenia o zapoznaniu się z dokumentami z zakresu ochrony danych osobowych, oświadczenia o odbyciu szkolenia z zakresu ochrony danych osobowych, oświadczenia o przestrzeganiu ochrony danych osobowych oraz ustalonych procedur

Załącznik 2. Wzór programu szkolenia wstępnego z zakresu ochrony danych osobowych

Załącznik 3. Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych

Załącznik 4. Wzór umowy powierzenia przetwarzania danych osobowych (SBM jako Administrator Danych Osobowych)

Załącznik 4a. Wzór umowy powierzenia przetwarzania danych osobowych (SBM jako Podmiot przetwarzający)

Załącznik 5. Wzór ewidencji podmiotów przetwarzających

Załącznik 6. Wzór rejestru kategorii czynności przetwarzania

Załącznik 7. Wzór rejestru żądań udostępnień danych osobowych

Załącznik 8. Wzór ewidencji obiektów

Załącznik 9. Wzór rejestru czynności przetwarzania danych osobowych

Załącznik 10. Wzór rejestru żądań osób fizycznych

Załącznik 11. Procedura zarządzania ryzykiem

Załącznik 12. Procedura nadawania i odbierania upoważnień do przetwarzania danych osobowych

Załącznik 13. Procedura realizacji prawa do uzyskania informacji

Załącznik 14. Procedura realizacji prawa dostępu do danych osobowych

Załącznik 15. Procedura realizacji prawa do sprostowania danych

Załącznik 16. Procedura realizacji prawa do usunięcia danych oraz prawa do bycia zapomnianym

Załącznik 17. Procedura realizacji prawa do ograniczenia przetwarzania

Załącznik 18. Procedura realizacji prawa do przenoszenia danych

Załącznik 19. Procedura realizacji prawa do sprzeciwu

Załącznik 20. Procedura realizacji prawa do cofnięcia zgody

Załącznik 21. Procedura postępowania w przypadku incydentów z zakresu ochrony danych osobowych

Załącznik 22. Procedura zgłaszania naruszeń ochrony danych osobowych do Urzędu Ochrony Danych Osobowych.

Załącznik 23. Procedura usuwania i niszczenia danych osobowych

u *Am*

2. W przypadku ewidencji i rejestrów Administrator Danych Osobowych może zastąpić wzory, które stanowią Załączniki do niniejszej Polityki, dedykowanym oprogramowaniem służącym do tych samych celów.

IX. POSTANOWIENIA KOŃCOWE


§ 36.

Postanowienia końcowe

1. W zakresie nieuregulowanym niniejszą Polityką znajdują zastosowanie powszechnie obowiązujące przepisy prawa, w szczególności dotyczące ochrony danych osobowych.
2. W przypadku zmiany stanu prawnego, która będzie skutkować niezgodnością niniejszej Polityki z prawem, postanowienie takie traci moc. Administrator Danych Osobowych podejmuje niezwłoczne działania na rzecz dostosowania niniejszej Polityki do nowego stanu prawnego.
3. Niniejsza Polityka może być zmieniona lub uchylona w takim samym trybie, w jakim została przyjęta.
4. Niniejsza Polityka obowiązuje od dnia 05.01.2021 r.

Wykaz zmian:

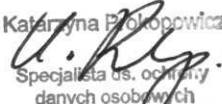
Edycja nr	Data edycji	Opis zmiany
2.0	05.01.2021	Całkowita zmiana treści z utrzymaniem założeń ogólnych i szczególnych


MACIEJ CZYŃSKI

PREZES ZARZĄDU
SBM „SKARBOWIEC”


ROBERT KRUPA

CZŁONEK ZARZĄDU
SBM „SKARBOWIEC”

Katarzyna Prokopowicz

Specjalista ds. ochrony
danych osobowych

SBM Skarbowiec	Nazwa dokumentu:			
	Oświadczenie			
	Edycja:	1	Obowiązuje od:	05.01.2021
	Uchwała nr	1/2021	Data uchwalenia:	05.01.2021
Zastępuje:	N/D			
<i>Własność SBM Skarbowiec. Do użytku wewnętrznego. Podlega nadzorowi.</i>				
Opracował		Zatwierdził		
Katarzyna Prokopowicz		Zarząd		

Warszawa, dnia r.

Oświadczenie

Ja, niżej podpisany/podpisana _____, oświadczam, że zostałem/zostałam zapoznany/zapoznana z następującymi dokumentami z zakresu ochrony danych osobowych:

- Polityka Bezpieczeństwa Ochrony Danych Osobowych w SBM Skarbowiec
- Instrukcja Zarządzania Systemem Informatycznym

Zobowiązuję się przestrzegać obowiązujących przepisów prawa z zakresu ochrony danych osobowych, Polityki Bezpieczeństwa Ochrony Danych Osobowych w SBM Skarbowiec, ustanowionych procedur, instrukcji i zasad, jak również zachować w tajemnicy — w czasie trwania umowy i po jej zakończeniu — wszystkie informacje, jakie uzyskałem/uzyskałam w trakcie wykonywania swoich obowiązków, w szczególności o danych osobowych, celach i sposobach ich przetwarzania oraz sposobach ich zabezpieczenia.

Zobowiązuję się przetwarzać dane osobowe zgodnie z nadanym upoważnieniem.

Zobowiązuję się nie wykorzystywać danych osobowych do innych celów niż uzgodnione z Administratorem Danych Osobowych i bez jego polecenia.

Oświadczam, że zostałem/zostałam poinformowany/poinformowana o odpowiedzialności za naruszenie przepisów z zakresu ochrony danych osobowych, Polityki Bezpieczeństwa Ochrony Danych Osobowych w SBM Skarbowiec, ustanowionych procedur, instrukcji i zasad.

Oświadczam również, że w dn. odbyłem/odbyłam szkolenie w zakresie ochrony danych osobowych i uzyskałem/uzyskałam niezbędne informacje i wskazówki do rzetelnego wykonywania pracy z poszanowaniem osób, których dane dotyczą.

 podpis

ROBERT KRUPA
 CZŁONEK ZARZĄDU
 SBM „SKARBOWIEC”

u *cu*

SBM Skarbowiec	Nazwa dokumentu: Wzór programu szkolenia wstępnego z zakresu ochrony danych osobowych			
	Edycja:	1	Obowiązuje od:	05.01.2021
	Uchwała nr	1/2021	Data uchwalenia:	05.01.2021
	Zastępuje:	N/D		
<i>Własność SBM Skarbowiec. Do użytku wewnętrznego. Podlega nadzorowi.</i>				
Opracował		Zatwierdził		
Katarzyna Prokopowicz		Zarząd		

Cel:

Celem dokumentu jest standaryzacja przeprowadzanych szkoleń z zakresu ochrony danych osobowych, które mają poprawić świadomość pracowników, w tym świadomość odpowiedzialności za czyny umyślne i nieumyślne, oraz zminimalizować ryzyko naruszeń ochrony danych osobowych.

Dotyczy: wszyscy nowoprzyjęci pracownicy/zleceniobiorcy, którzy przetwarzają dane osobowe

Osoba odpowiedzialna: Inspektor Ochrony Danych

Wytyczne:

- 1) Szkolenie odbywa się przed dopuszczeniem nowozatrudnionego pracownika/zleceniobiorcy do pracy.
- 2) Szkolenie dotyczy wszystkich pracowników zatrudnionych i/lub pracujących na zlecenie SBM Skarbowiec, bez względu na podstawę i formę zatrudnienia.
- 3) Za przeprowadzenie szkolenia jest odpowiedzialny bezpośredni przełożony nowozatrudnionego pracownika.
- 4) Szkolenie odbywa się zgodnie z ramowym programem szkolenia wstępnego z zakresu ochrony danych osobowych i trwa 2 godziny zegarowe.

05.01.2021 r.

Katarzyna Prokopowicz


ROBERT KRUPA

CZŁONEK ZARZĄDU
SBM „SKARBOWIEC”





- 5) W szczególnych przypadkach czas trwania szkolenia może zostać skrócony, jednak szkolenie nie powinno trwać krócej niż 1 godzina zegarowa.
- 6) Po odbyciu szkolenia pracownik potwierdza ten fakt złożeniem własnoręcznego podpisu oraz wpisaniem daty szkolenia na Oświadczeniu.

Ramowy program szkolenia:

Lp.	Zakres tematyczny	Wymiar godz.
1.	Główne definicje związane z ochroną danych osobowych. System ochrony danych osobowych w SBM Skarbowiec. SBM Skarbowiec jako administrator.	0:15
2.	Zasady przetwarzania danych osobowych oraz prawa osób, których dane dotyczą. Podstawy prawne przetwarzania danych osobowych (art. 6 ust. 1, art. 9 ust. 2 RODO). Odpowiedzialność pracownika upoważnionego do przetwarzania danych osobowych.	0:20
3.	Uczestnik szkolenia jako przedstawiciel/pracownik – obowiązki i prawa SBM Skarbowiec.	0:10
4.	Wytyczne: <ul style="list-style-type: none"> • Procedury związane z ochroną danych osobowych. • Przetwarzanie danych osobowych w poszczególnych działach. • Przykłady przetwarzania danych osobowych. • Algorytmy postępowania z danych dla poszczególnych działów. • Dokumentacja wymagana przy zatrudnieniu nowego pracownika. 	1:15
Razem		2:00

Wykaz zmian:

Edycja nr	Data edycji	Opis zmiany

k *am*

Krupa
ROBERT KRUPA
 CZŁONEK ZARZĄDU
 SBM „SKARBOWIEC”

Nazwa dokumentu: SBM Skarbowiec				
Ewidencja osób upoważnionych do przetwarzania danych osobowych		Obowiązuje od: 05.01.2021	Data uchwalenia: 05.01.2021	
Edycja: 1	Uchwała nr 1./2021			
Zastępuje: N/D	Własność SBM Skarbowiec. Do użytku wewnętrznego. Podlega nadzorowi.			
Opracował Katarzyna Prokopowicz		Zatwierdził Zarząd		
Imię	Nazwisko	Data nadania upoważnienia	Osoba nadająca upoważnienie	Data ustania upoważnienia


ROBERT KRUPA
 CZŁONEK ZARZĄDU
 SBM „SKARBOWIEC”

[Handwritten mark]

SBM Skarbowiec	Nazwa dokumentu: Wzór umowy powierzenia przetwarzania danych osobowych (SBM Skarbowiec jako Administrator)			
	Edycja:	1	Obowiązuje od:	05.01.2021
	Uchwała nr	1/2021	Data uchwalenia:	05.01.2021
	Zastępuje:	N/D		
<i>Własność SBM Skarbowiec. Do użytku wewnętrznego. Podlega nadzorowi.</i>				
Opracował		Zatwierdził		
Katarzyna Prokopowicz		Zarząd		

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta dnia r. pomiędzy:

(zwana dalej „Umową”)

Spółdzielnią Budowlano-Mieszkaniową „Skarbowiec” z siedzibą w Warszawie, ul. Grójecka 41, 02-031 Warszawa, wpisaną do Krajowego Rejestru Sądowego przez Sąd Rejonowy dla m. st. Warszawy pod numerem KRS 0000410983, REGON 000490547, NIP 5250007046.

zwanym(-ną) w dalszej części Umowy „**Administratorem danych**” lub „**Administratorem**”,
reprezentowanym(-ną) przez:

a

_____ [dane podmiotu, który zawiera Umowę]

zwanym(-ną) w dalszej części Umowy „**Podmiotem przetwarzającym**”,
reprezentowanym(-ną) przez:

a u

§1. Powierzenie przetwarzania danych osobowych

1. Administrator danych powierza Podmiotowi przetwarzającemu dane osobowe do przetwarzania w trybie art. 28 ogólnego 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 (Dz.Urz.UE.L Nr 119, str. 1) (zwanego w dalszej części Umowy „Rozporządzeniem”), na zasadach, w zakresie i w celu określonych w niniejszej Umowie.
2. Podmiot przetwarzający zobowiązuje się do przetwarzania powierzonych mu danych osobowych zgodnie z niniejszą Umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, chroniącymi prawa osób, których dane dotyczą.

§2. Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał powierzone na podstawie Umowy dane [należy podać rodzaj danych, tj. tzw. dane zwykłe oraz dane szczególnych kategorii] dotyczące [należy podać kategorię osób, których dane dotyczą, np. pracowników administratora, klientów administratora itd.] w zakresie [należy podać kategorie danych osobowych, np. imiona i nazwiska, adresy zamieszkania, numery PESEL itd.].
2. Dane osobowe powierzone przez Administratora danych będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu [należy podać cel przetwarzania danych przez Podmiot przetwarzający, np. realizacji umowy z dnia nr w zakresie prowadzenia spraw kadrowych].
3. Podmiot przetwarzający jest upoważniony do wykonywania następujących czynności przetwarzania powierzonych danych: 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 [należy wybrać właściwe] – które są w minimalnym zakresie niezbędne do realizacji celu, o którym mowa w ust. 2 powyżej.

§3. Obowiązki Podmiotu przetwarzającego

1. Podmiot przetwarzający przy przetwarzaniu powierzonych danych osobowych zobowiązuje się do ich zabezpieczenia przez stosowanie odpowiednich środków technicznych i organizacyjnych, odpowiadających stanowi wiedzy technicznej, zapewniających zgodność z Rozporządzeniem, w tym adekwatny stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób, których dane dotyczą. Lista środków technicznych i organizacyjnych stosowanych przez Podmiot przetwarzający stanowi załącznik nr 1 do Umowy.
2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane osobowe, przy czym będą to jedynie osoby, które mają odpowiednie przeszkolenie z zakresu ochrony danych osobowych i są niezbędne do realizacji celu niniejszej Umowy.
4. Podmiot przetwarzający zapewnia, że osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej Umowy, zobowiążą się do zachowania tajemnicy lub będą podlegali odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy, o której mowa w

u An

art. 28 ust. 3 lit. b Rozporządzenia, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu. Podmiot przetwarzający zapewnia ponadto, że osoby, o których mowa w niniejszym ustępie, będą przetwarzały dane osobowe zgodnie z zasadą wiedzy koniecznej.

5. Dla prawidłowej realizacji ust. 4 Podmiot Przetwarzający dokonuje okresowej weryfikacji listy osób, którym udzielono dostępu do danych przetwarzanych w imieniu Administratora.
6. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem niezwłocznie usuwa/zwraca Administratorowi wszelkie dane osobowe *[należy wybrać, czy Podmiot przetwarzający ma usunąć, czy zwrócić dane]* oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
7. Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osób, których dane dotyczą, oraz z obowiązków określonych w art. 32–36 Rozporządzenia. Podmiot przetwarzający – w razie wpływu do niego żądania w zakresie realizacji praw osób, których dotyczą powierzone dane – informuje o tym Administratora w terminie 5 dni roboczych od otrzymania wiadomości *[Administrator termin może określić dowolnie, z zastrzeżeniem terminowej realizacji zadań wynikających z Rozporządzenia]*. Udzielając informacji, Podmiot przetwarzający przekazuje dane nadawcy i treść żądania oraz określa, w jakim zakresie jest w stanie przyczynić się do realizacji żądania.
8. W przypadku stwierdzenia jakiegokolwiek naruszenia ochrony danych osobowych Podmiot przetwarzający lub podwykonawca Podmiotu przetwarzającego zgłasza je Administratorowi w ciągu 24 godzin.

§4. Prawo kontroli

1. Zgodnie z art. 28 ust. 3 lit. h Rozporządzenia Administrator danych ma prawo kontroli, mającej na celu weryfikację, czy Podmiot przetwarzający spełnia obowiązki wynikające z niniejszej Umowy.
2. Administrator danych będzie realizować prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum 7-dniowym uprzedzeniem.
3. Prawo do przeprowadzenia kontroli obejmuje: wstęp do pomieszczeń, w których znajdują się zasoby uczestniczące w operacjach przetwarzania powierzonych danych osobowych; żądanie złożenia pisemnych lub ustnych wyjaśnień od osób upoważnionych do przetwarzania powierzonych danych osobowych; wgląd do wszelkich dokumentów i wszelkich danych mających bezpośredni związek z celem kontroli; przeprowadzanie oględzin urządzeń, nośników oraz systemów informatycznych służących do przetwarzania powierzonych danych.
4. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych, nie dłuższym niż 7 dni.
5. Powyżej określone zasady kontroli Podmiotu Przetwarzającego mają zastosowanie do przeprowadzanych przez Administratora kontroli podwykonawców Podmiotu przetwarzającego, o których mowa w § 6 ust. 1 Umowy.

u au

§5. Raportowanie

1. Na wniosek Administratora Podmiot przetwarzający udostępnia wszelkie informacje niezbędne do realizacji lub wykazania spełnienia obowiązków wynikających z Rozporządzenia.
2. Informacji, o których mowa w ust. 1, udziela się w terminie 15 dni roboczych od dnia doręczenia wniosku, z zastrzeżeniem ust. 3.
3. Jeżeli wniosek, o którym mowa w ust. 1, dotyczy realizacji obowiązku zgłoszenia naruszenia ochrony danych osobowych lub usunięcia jego skutków, Podmiot przetwarzający udziela informacji w najbliższym możliwym terminie, nie później niż w ciągu 24 godzin od doręczenia wniosku.

§6. Dalsze powierzenie danych do przetwarzania

1. Administrator wyraża zgodę na powierzenie danych osobowych objętych niniejszą Umową do dalszego przetwarzania przez podwykonawców Podmiotu przetwarzającego, w celu wykonania niniejszej Umowy, przy czym podwykonawcy Podmiotu przetwarzającego powinni spełniać te same gwarancje i obowiązki, jakie zostały nałożone na Podmiot przetwarzający niniejszą Umową. Lista takich podmiotów (podprocesorów) stanowi załącznik nr 2 do Umowy.
2. W przypadku zmiany lub dodania innych podwykonawców biorących udział w przetwarzaniu danych powierzonych przez Administratora Podmiot przetwarzający informuje o zamierzonych zmianach, dając Administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian w terminie 5 dni roboczych od przekazania informacji o zamierzonych zmianach.
3. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na udokumentowane polecenie Administratora danych, chyba że taki obowiązek nakłada na Podmiot przetwarzający prawo Unii Europejskiej lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora danych o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
4. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązanie się z obowiązków spoczywających na podwykonawcy, wynikających z niniejszej Umowy.

§7. Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią Umowy, a w szczególności za udostępnienie osobom nieupoważnionym powierzonych do przetwarzania danych osobowych.
2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w Umowie, o jakiegokolwiek decyzji administracyjnej lub jakimkolwiek orzeczeniu dotyczących przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Prezesa Urzędu Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora danych.

u. Am

§8. Czas obowiązywania Umowy

1. Niniejsza Umowa obowiązuje od dnia jej zawarcia przez czas *nieokreślony/określony od do* [należy wybrać].
2. Każda ze stron może wypowiedzieć niniejszą Umowę z zachowaniem jednomiesięcznego okresu wypowiedzenia.

§9. Rozwiązanie Umowy

Administrator danych może rozwiązać niniejszą Umowę ze skutkiem natychmiastowym, gdy Podmiot przetwarzający:

- a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie,
- b) przetwarza dane osobowe w sposób niezgodny z Umową,
- c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych.

§10. Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora danych i od współpracujących z nim osób, a także danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy, w formie ustnej, pisemnej lub elektronicznej („dane poufne”).
2. Podmiot przetwarzający oświadcza, że w związku z zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora danych w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.

§11. Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.
2. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
3. Sędem właściwym dla rozpatrzenia sporów wynikających z niniejszej Umowy będzie sąd właściwy Administratora danych.

Administrator danych

Podmiot przetwarzający

Załączniki:

Załącznik nr 1 – Sprawdzenie podmiotu przetwarzającego

Załącznik nr 2 – Wykaz podwykonawców Podmiotu przetwarzającego (subprocesorów)


ROBERT KRUPA

CZŁONEK ZARZĄDU
SBM „SKARBOWIEC”



Załącznik nr 1. Sprawdzenie podmiotu przetwarzającego

Lp.	Pytanie	Odpowiedź	Wyjaśnienie (jeśli konieczne)
1.	Czy osoby przetwarzające dane osobowe zapoznały się z treścią rozporządzenia o ochronie danych osobowych z dn. 27 kwietnia 2016 r. lub odbyły stosowane szkolenie w tym zakresie?		
2.	Czy osoby przetwarzające dane posiadają stosowane upoważnienia?		
3.	Czy podmiot przetwarzający powołał Inspektora Ochrony Danych (IOD)?		
4.	Jeżeli podmiot przetwarzający nie powołał IOD to czy wyznaczył osobę odpowiedzialną za zapewnianie nadzoru nad systemem ochrony danych osobowych?		
5.	Czy podmiot wdrożył Politykę Bezpieczeństwa Ochrony Danych Osobowych i ją aktualizuje?		
6.	Czy podmiot wdrożył Instrukcję Zarządzania Systemem Informatycznym i ją aktualizuje?		
7.	Czy podmiot przetwarzający zleca wykonanie czynności podwykonawcom stosując dalsze podpowieranie danych?		
8.	Czy podmiot przetwarzający przekazuje dane poza teren Europejskiego Obszaru Gospodarczego? <i>(proszę uwzględnić miejsce przechowywania serwerów)</i>		
9.	Czy zabezpieczenia organizacyjne i techniczne gwarantują bezpieczeństwo i poufność danych?		
10.	Jeśli tak – jakie kryteria zapewnienia bezpieczeństwa i poufności zastosowano: 1. pseudonimizację, 2. szyfrowanie, 3. zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów, 4. zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu technicznego i/lub fizycznego?		

.....
(podpis osoby upoważnionej)


ROBERT KRUPA

CZŁONEK ZARZĄDU
SBM „SKARBOWIEC”



Załącznik nr 2. Wykaz podwykonawców Podmiotu przetwarzającego (subprocesorów)

Przy wykonaniu Umowy Procesor korzysta z usług następujących subprocesorów:

NAZWA I DANE SUBPROCESORA	CEL PODPOWIERZENIA	ZAKRES DANYCH

Am



ROBERT KRUPA

CZŁONEK ZARZĄDU
SBM „SKARBOWIEC”

SBM Skarbowiec	Nazwa dokumentu: Wzór umowy powierzenia przetwarzania danych osobowych (SBM Skarbowiec jako Podmiot przetwarzający)			
	Edycja:	1	Obowiązuje od:	05.01.2021
	Uchwała nr	1/2021	Data uchwalenia:	05.01.2021
	Zastępuje:	N/D		
<i>Własność SBM Skarbowiec. Do użytku wewnętrznego. Podlega nadzorowi.</i>				
Opracował		Zatwierdził		
Katarzyna Prokopowicz		Zarząd		

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta dnia r. pomiędzy:

(zwana dalej „Umową”)

_____ [dane podmiotu, który zawiera Umowę]

zwanym(-ną) w dalszej części Umowy „**Administratorem danych**” lub „**Administratorem**”,
reprezentowanym(-ną) przez:

a

Spółdzielnię Budowlano-Mieszkaniową „Skarbowiec” z siedzibą w Warszawie, ul. Grójecka 41, 02-031 Warszawa, wpisaną do Krajowego Rejestru Sądowego przez Sąd Rejonowy dla m. st. Warszawy pod numerem KRS 0000410983, REGON 000490547, NIP 5250007046.

zwanym(-ną) w dalszej części Umowy „**Podmiotem przetwarzającym**”
reprezentowanym(-ną) przez:

Am

u

§1. Powierzenie przetwarzania danych osobowych

1. Administrator danych powierza Podmiotowi przetwarzającemu dane osobowe do przetwarzania w trybie art. 28 ogólnego 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 (Dz.Urz.UE.L Nr 119, str. 1) (zwanego w dalszej części Umowy „Rozporządzeniem”), na zasadach, w zakresie i w celu określonych w niniejszej Umowie.
2. Podmiot przetwarzający zobowiązuje się do przetwarzania powierzonych mu danych osobowych zgodnie z niniejszą Umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, chroniącymi prawa osób, których dane dotyczą.

§2. Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał powierzone na podstawie Umowy dane [należy podać rodzaj danych, tj. tzw. dane zwykłe oraz dane szczególnych kategorii] dotyczące [należy podać kategorię osób, których dane dotyczą, np. pracowników administratora, klientów administratora itd.] w zakresie [należy podać kategorie danych osobowych, np. imiona i nazwiska, adresy zamieszkania, numery PESEL itd.].
2. Dane osobowe powierzone przez Administratora danych będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu [należy podać cel przetwarzania danych przez Podmiot przetwarzający, np. realizacji umowy z dnia nr w zakresie prowadzenia spraw kadrowych].
3. Podmiot przetwarzający jest upoważniony do wykonywania następujących czynności przetwarzania powierzonych danych: 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 [należy wybrać właściwe] – które są w minimalnym zakresie niezbędne do realizacji celu, o którym mowa w ust. 2 powyżej.

§3. Obowiązki Podmiotu przetwarzającego

1. Podmiot przetwarzający przy przetwarzaniu powierzonych danych osobowych zobowiązuje się do ich zabezpieczenia przez stosowanie odpowiednich środków technicznych i organizacyjnych, odpowiadających stanowi wiedzy technicznej, zapewniających zgodność z Rozporządzeniem, w tym adekwatny stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób, których dane dotyczą. Lista środków technicznych i organizacyjnych stosowanych przez Podmiot przetwarzający stanowi załącznik nr 1 do Umowy.
2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane osobowe, przy czym będą to jedynie osoby, które mają odpowiednie przeszkolenie z zakresu ochrony danych osobowych i są niezbędne do realizacji celu niniejszej Umowy.
4. Podmiot przetwarzający zapewnia, że osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej Umowy, zobowiążą się do zachowania tajemnicy lub będą podlegali odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy, o której mowa w

Ar

u

art. 28 ust. 3 lit. b Rozporządzenia, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu. Podmiot przetwarzający zapewnia ponadto, że osoby, o których mowa w niniejszym ustępie, będą przetwarzały dane osobowe zgodnie z zasadą wiedzy koniecznej.

5. Dla prawidłowej realizacji ust. 4 Podmiot Przetwarzający dokonuje okresowej weryfikacji listy osób, którym udzielono dostępu do danych przetwarzanych w imieniu Administratora.
6. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem niezwłocznie usuwa/zwraca Administratorowi wszelkie dane osobowe [należy wybrać, czy Podmiot przetwarzający ma usunąć, czy zwrócić dane] oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
7. Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osób, których dane dotyczą, oraz z obowiązków określonych w art. 32–36 Rozporządzenia. Podmiot przetwarzający – w razie wpływu do niego żądania w zakresie realizacji praw osób, których dotyczą powierzone dane – informuje o tym Administratora w terminie 5 dni roboczych od otrzymania wiadomości [Administrator termin może określić dowolnie, z zastrzeżeniem terminowej realizacji zadań wynikających z Rozporządzenia]. Udzielając informacji, Podmiot przetwarzający przekazuje dane nadawcy i treść żądania oraz określa, w jakim zakresie jest w stanie przyczynić się do realizacji żądania.
8. W przypadku stwierdzenia jakiegokolwiek naruszenia ochrony danych osobowych Podmiot przetwarzający lub podwykonawca Podmiotu przetwarzającego zgłasza je Administratorowi w ciągu 24 godzin.

§4. Prawo kontroli

1. Zgodnie z art. 28 ust. 3 lit. h Rozporządzenia Administrator danych ma prawo kontroli, mającej na celu weryfikację, czy Podmiot przetwarzający spełnia obowiązki wynikające z niniejszej Umowy.
2. Administrator danych będzie realizować prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum 7-dniowym uprzedzeniem.
3. Prawo do przeprowadzenia kontroli obejmuje: wstęp do pomieszczeń, w których znajdują się zasoby uczestniczące w operacjach przetwarzania powierzonych danych osobowych; żądanie złożenia pisemnych lub ustnych wyjaśnień od osób upoważnionych do przetwarzania powierzonych danych osobowych; wgląd do wszelkich dokumentów i wszelkich danych mających bezpośredni związek z celem kontroli; przeprowadzanie oględzin urządzeń, nośników oraz systemów informatycznych służących do przetwarzania powierzonych danych.
4. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych, nie dłuższym niż 7 dni.
5. Powyżej określone zasady kontroli Podmiotu Przetwarzającego mają zastosowanie do przeprowadzanych przez Administratora kontroli podwykonawców Podmiotu przetwarzającego, o których mowa w § 6 ust. 1 Umowy.

§5. Raportowanie

1. Na wniosek Administratora Podmiot przetwarzający udostępnia wszelkie informacje niezbędne do realizacji lub wykazania spełnienia obowiązków wynikających z Rozporządzenia.

Ar

h

2. Informacji, o których mowa w ust. 1, udziela się w terminie 15 dni roboczych od dnia doręczenia wniosku, z zastrzeżeniem ust. 3.
3. Jeżeli wniosek, o którym mowa w ust. 1, dotyczy realizacji obowiązku zgłoszenia naruszenia ochrony danych osobowych lub usunięcia jego skutków, Podmiot przetwarzający udziela informacji w najbliższym możliwym terminie, nie później niż w ciągu 24 godzin od doręczenia wniosku.

§6. Dalsze powierzenie danych do przetwarzania

1. Administrator wyraża zgodę na powierzenie danych osobowych objętych niniejszą Umową do dalszego przetwarzania przez podwykonawców Podmiotu przetwarzającego, w celu wykonania niniejszej Umowy, przy czym podwykonawcy Podmiotu przetwarzającego powinni spełniać te same gwarancje i obowiązki, jakie zostały nałożone na Podmiot przetwarzający niniejszą Umową.
2. W przypadku zmiany lub dodania innych podwykonawców biorących udział w przetwarzaniu danych powierzonych przez Administratora Podmiot przetwarzający informuje o zamierzonych zmianach, dając Administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian w terminie 5 dni roboczych od przekazania informacji o zamierzonych zmianach.
3. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na udokumentowane polecenie Administratora danych, chyba że taki obowiązek nakłada na Podmiot przetwarzający prawo Unii Europejskiej lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora danych o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
4. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązanie się z obowiązków spoczywających na podwykonawcy, wynikających z niniejszej Umowy.

§7. Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią Umowy, a w szczególności za udostępnienie osobom nieupoważnionym powierzonych do przetwarzania danych osobowych.
2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w Umowie, o jakiegokolwiek decyzji administracyjnej lub jakimkolwiek orzeczeniu dotyczących przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Prezesa Urzędu Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora danych.

§8. Czas obowiązywania Umowy

1. Niniejsza Umowa obowiązuje od dnia jej zawarcia przez czas *nieokreślony/określony od do* [należy wybrać].

Ar

h

2. Każda ze stron może wypowiedzieć niniejszą Umowę z zachowaniem jednomiesięcznego okresu wypowiedzenia.

§9. Rozwiązanie Umowy

Administrator danych może rozwiązać niniejszą Umowę ze skutkiem natychmiastowym, gdy Podmiot przetwarzający:

- a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie,
- b) przetwarza dane osobowe w sposób niezgodny z Umową,
- c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych.

§10. Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora danych i od współpracujących z nim osób, a także danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy, w formie ustnej, pisemnej lub elektronicznej („dane poufne”).
2. Podmiot przetwarzający oświadcza, że w związku z zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora danych w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.

§11. Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.
2. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
3. Sędem właściwym dla rozpatrzenia sporów wynikających z niniejszej Umowy będzie sąd właściwy Administratora danych.

Administrator danych

Podmiot przetwarzający

Załączniki:

Załącznik nr 1 – Sprawdzenie podmiotu przetwarzającego

Załącznik nr 2 – Wykaz podwykonawców Podmiotu przetwarzającego (subprocesorów)

MACIEJ CZYŃSKI

PREZES-ZARZĄDU
SBM „SKARBOWIEC”

ROBERT KRUPA

CZŁONEK ZARZĄDU
SBM „SKARBOWIEC”

Załącznik nr 1. Sprawdzenie podmiotu przetwarzającego

Lp.	Pytanie	Odpowiedź	Wyjaśnienie (jeśli konieczne)
1.	Czy osoby przetwarzające dane osobowe zapoznały się z treścią rozporządzenia o ochronie danych osobowych z dn. 27 kwietnia 2016 r. lub odbyły stosowane szkolenie w tym zakresie?	TAK	
2.	Czy osoby przetwarzające dane posiadają stosowane upoważnienia?	TAK	
3.	Czy podmiot przetwarzający powołał Inspektora Ochrony Danych (IOD)?	TAK	
4.	Jeżeli podmiot przetwarzający nie powołał IOD to czy wyznaczył osobę odpowiedzialną za zapewnianie nadzoru nad systemem ochrony danych osobowych?	N/D	
5.	Czy podmiot wdrożył Politykę Bezpieczeństwa Ochrony Danych Osobowych i ją aktualizuje?	TAK	
6.	Czy podmiot wdrożył Instrukcję Zarządzania Systemem Informatycznym i ją aktualizuje?	TAK	
7.	Czy podmiot przetwarzający zleca wykonanie czynności podwykonawcom stosując dalsze podpowieranie danych?	TAK	
8.	Czy podmiot przetwarzający przekazuje dane poza teren Europejskiego Obszaru Gospodarczego? <i>(proszę uwzględnić miejsce przechowywania serwerów)</i>	TAK	Microsoft – na mocy standardowych klauzul umownych
9.	Czy zabezpieczenia organizacyjne i techniczne gwarantują bezpieczeństwo i poufność danych?	TAK	
10.	Jeśli tak – jakie kryteria zapewnienia bezpieczeństwa i poufności zastosowano: 1. pseudonimizację, 2. szyfrowanie, 3. zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów, 4. zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu technicznego i/lub fizycznego?	1, 3, 4	

.....
(podpis osoby upoważnionej)

MACIEJ CZYŃSKI

PREZES ZARZĄDU
SBM „SKARBOWIEC”

ROBERT KRUPA

CZŁONEK ZARZĄDU
SBM „SKARBOWIEC”

SBM Skarbowiec	Nazwa dokumentu: Ewidencja osób upoważnionych do przetwarzania danych osobowych			
	Edycja:	1	Obowiązuje od:	05.01.2021
	Uchwała nr	1/.2021	Data uchwalenia:	05.01.2021
	Zastępuje:	N/D		
<i>Własność SBM Skarbowiec. Do użytku wewnętrznego. Podlega nadzorowi.</i>				
Opracował		Zatwierdził		
Katarzyna Prokopowicz		Zarząd		

Nazwa Podmiotu przetwarzającego	Dane kontaktowe do IOD	Charakter powierzenia	Zakres powierzonych danych	Data podpisania umowy powierzenia	Data rozwiązania umowy powierzenia


ROBERT KRUPA

CZŁONEK ZARZĄDU
SBM „SKARBOWIEC”



SBM Skarbowiec

Rejestr kategorii czynności przetwarzania

Nazwa i dane kontaktowe przetwarzającego	
Nazwa	Spółdzielnia Budowlano-Mieszkaniowa "Skarbowiec"
Adres	ul. Grójecka 41, 02-031 Warszawa
Email	zarzad@skarbowiec.waw.pl
Telefon	

Data ostatniej aktualizacji	dd.mm.rrrr
-----------------------------	------------

Am

h

SBM		Nazwa dokumentu:	
Skarbowiec		Relester kategorii czynności przetwarzania	
Edycja:	1	Obowiązuje od:	05.01.2021
Liczbowa nr:	1/2021	Data uchwalenia:	05.01.2021
Zastępuje:	N/D		
Własność SBM Skarbowiec. Do użytku wewnętrznego. Podlega nadzorowi.			
Opracował:	Zatwierdził:		
Katarzyna Prokopowicz	Zarząd		

LP	Kategorie przetwarzania	Opisowy opis techniczny i organizacyjny środków bezpieczeństwa (cały tekst to read-only)	Administrator					Ciepłota przetwarzania	Nowy punkt, przedział lub organizacja przydzielona do tegoż danej w procedurze	Dotyczy to informacji o bezpieczeństwie przetwarzania (inne niż dane)	Podprzetwarzający (podwykonawca) - jeśli dotyczy	
			Nazwa i dane kontaktowe administratora	Nazwa i dane kontaktowe wydziału/instytucji (jeśli dotyczy)	Nazwa i dane kontaktowe jednostki wykonawczej (jeśli występuje)	Instytucja odbiorcy danych (jeśli powstano)	Nazwa i dane kontaktowe podprzetwarzającego (podwykonawcy)				Kategorie przetwarzanych danych	
1	Art. 30 ust. 2 lit. b	Art. 30 ust. 2 lit. d, art. 33 ust. 1		Art. 30 ust. 2 lit. a				Art. 30 ust. 2 lit. c	Art. 30 ust. 2 lit. c			
2												

Em


ROBERT KRUPA
 CZŁONEK ZARZĄDU
 SBM „SKARBOWIEC”

Nazwa dokumentu:		Rejestr żądań udostępnienia danych osobowych			
SBM Skarbowiec		Edycja:	1	Obowiązuje od:	05.01.2021
		Uchwała nr	1./2021	Data uchwalenia:	05.01.2021
		Zastępuje:	N/D		
<i>Własność SBM Skarbowiec. Do użytku wewnętrznego. Podlega nadzorowi.</i>					
Opracował		Zatwierdził			
Katarzyna Prokopowicz		Zarząd			

Odbiorca danych	Data żądania udostępnienia danych	Zakres udostępnienia danych	Data udostępnienia danych	Osoba udostępniająca dane

[Signature]
ROBERT KRUPA
 CZŁONEK ZARZĄDU
 SBM „SKARBOWIEC”

[Signature]

SBM Skarbowiec	Nazwa dokumentu: Ewidencja obszarów przetwarzania danych			
	Edycja:	1	Obowiązuje od:	05.01.2021
	Uchwała nr	1./2021	Data uchwalenia:	05.01.2021
	Zastępuje:	N/D		
<i>Własność SBM Skarbowiec. Do użytku wewnętrznego. Podlega nadzorowi.</i>				
Opracował		Zatwierdził		
Katarzyna Prokopowicz		Zarząd		

Ewidencja obszarów - data ostatniej aktualizacji: dd.mm.rrrr			
Nazwa obszaru	Adres	Zakres danych	Opis zabezpieczeń

An


ROBERT KRUPA
CZŁONEK ZARZĄDU
SBM „SKARBOWIEC”

Rejestr czynności przetwarzania

SBM Skarbowiec	Nazwa dokumentu:			
	Wzór rejestru czynności przetwarzania			
	Edycja:	1	Obowiązuje od:	05.01.2021
	Uchwała nr	1/2021	Data uchwalenia:	05.01.2021
Zastępuje:	N/D			
<i>Własność SBM Skarbowiec. Do użytku wewnętrznego. Podlega nadzorowi.</i>				
Opracował		Zatwierdził		
Katarzyna Prokopowicz		Zarząd		

nazwa skrócona: **Proces**

1. Podmiot odpowiedzialny

nazwa (pełna) podmiotu odpowiedzialnego	Spółdzielnia Budowlano-Mieszkaniowa „Skarbowiec”
adres firmy	ul. Grójecka 41 02-031 Warszawa
NIP	525 000 70 46
adres email	zarzad@skarbowiec.waw.pl
nr telefonu	
zarząd / kierownictwo spółki	Maciej Czyński – Prezes Zarządu Tomasz Giller – Wiceprezes Robert Krupa – Członek Zarządu
kierownictwo działu IT nazwisko, imię nr telefonu adres email	



Rejestr czynności przetwarzania

2. dane procesu

nazwa procesu	
osoba kontaktowa	
nazwa skrócona procesu	
stan (data)	
Czy będą przetwarzane dane osobowe?	<input type="checkbox"/> tak <input type="checkbox"/> nie – jeśli nie, uzupełnić punkt „Opis narzędzia IT”.
Opis narzędzia IT:	



w przypadku przetwarzania danych powierzonych: dane kontaktowe podmiotu przetwarzającego nazwa bądź imię i nazwisko: adres: nr telefonu: e-mail:	
---	--

3. Cel

cel przetwarzania danych	nr	cel (szczegółowe dane)
	1	
	2	
	3	
	4	
podstawa prawna przetwarzania danych	<input type="checkbox"/>	umowa, stosunek zaufania podobny umowie (Art. 6 ust. 1b)
	<input type="checkbox"/>	poszanowanie zobowiązań prawnych (Art. 6 ust. 1 c)
	<input type="checkbox"/>	wyważenie interesów (Art. 6 ust. 1 f)
	<input type="checkbox"/>	zgoda osoby, której dane dotyczą (Art. 6 ust. 1 a) potwierdzenie:
	<input type="checkbox"/>	żywotne interesy osoby, której dane dotyczą (Art. 6 ust. 1 d)



u

Ca

Rejestr czynności przetwarzania

4. Osoby, których dane dotyczą i dane osobowe

kategorie osób, których dane dotyczą	<input type="checkbox"/>		
	<input type="checkbox"/>		
	<input type="checkbox"/>		
	<input type="checkbox"/>		
	<input type="checkbox"/>	inni	
przestrzeganie praw osób, których dane dotyczą	<input type="checkbox"/>	zbieranie u osoby, której dane dotyczą	
	<input type="checkbox"/>	osoba, której dane dotyczą, została poinformowana o przetwarzaniu jej danych	
	<input type="checkbox"/>	uzyskano zgodę osoby, której dane dotyczą	
	<input type="checkbox"/>		
kategorie danych osobowych	nr	grupy osób, których dane dotyczą	kategorie danych osobowych
	1		
	2		
	3		
	4		



Ar

U

Rejestr czynności przetwarzania

5. Odbiorca danych osobowych

wewnętrzny dostęp/odbiorca: kategorie osób mających dostęp w podmiocie przetwarzającym dane	osoba uprawniona / odbiorca	cel	kategorie danych
zewnątrzny dostęp/odbiorca: kategorie osób mających dostęp w podmiocie przetwarzającym dane			
transfer danych za granicę (UE, upoważnione państwa)	nazwa państwa / kategorie danych:		
transfer danych do państw trzecich	nazwa państwa / zobowiązanie umowne:		

6. Zainstalowane oprogramowanie lub systemy TI

nazwa	producent	opis działania	pochodzenie
			<input type="checkbox"/> własne rozwiązanie / indywidualne oprogramowanie <input type="checkbox"/> oprogramowanie standardowe lub zakupione <input type="checkbox"/> Cloud-Service
			<input type="checkbox"/> własne rozwiązanie / indywidualne oprogramowanie <input type="checkbox"/> oprogramowanie standardowe lub zakupione <input type="checkbox"/> Cloud-Service
			<input type="checkbox"/> własne rozwiązanie / indywidualne oprogramowanie <input type="checkbox"/> oprogramowanie standardowe lub zakupione <input type="checkbox"/> Cloud-Service

Rejestr czynności przetwarzania

7. Okresy usuwania danych

terminy blokowania i usuwania danych	kategoria danych (nr/nazwa)	terminy blokowania i usuwania danych
uzasadnienie, w jaki sposób zagwarantowane jest względnie zablokowanie lub usunięcie		
w jaki sposób kontrolowana jest skuteczność (rejstry blokowania/usuwania)		

8. Szczegółowa analiza ryzyka

scenariusz wystąpienia szkody	kategorie danych	istniejące środki ochronne

Cm

Rejestr czynności przetwarzania

9. Analiza ryzyka

Identyfikacja wymogu ochrony i ocena scenariuszy szkód

kategorie danych osobowych ❶	poz. A-E ❷	punkty	atributy ❸			wynik ❹
			C	I	A	

wynik: środki ochrony danych należy podzielić na następujące kategorie:

- poziom normalny
- poziom wysoki
- poziom bardzo wysoki.



10. Proceduralne środki ochrony danych

techniczne i organizacyjne środki zgodnie z art. 32 ust. 1 RODO

Cu

u

Rejestr czynności przetwarzania

11. Ocena skutków dla ochrony danych

Czy rodzaj, zakres i cel przetwarzania danych może skutkować powstaniem wysokiego ryzyka naruszenia praw osobistych i wolności osób, których dane dotyczą? Art. 35	<input type="checkbox"/> tak <input type="checkbox"/> nie
Czy w wyniku przetwarzania danych można dokonać oceny, na podstawie której podejmowane są prawnie wiążące decyzje przeciwko osobie, których dane dotyczą?	<input type="checkbox"/> tak <input type="checkbox"/> nie
Czy wrażliwe dane (art. 9) będą przetwarzane w szerokim zakresie?	<input type="checkbox"/> tak <input type="checkbox"/> nie
Czy chodzi o monitoring?	<input type="checkbox"/> tak <input type="checkbox"/> nie



Podsumowanie

Wnioski ogólne:	
wymóg oceny skutków dla ochrony danych	<input type="checkbox"/> tak <input type="checkbox"/> nie
zatwierdzono	

MACIEJ CZYŃSKI

PREZES ZARZĄDU
SBM „SKARBOWIEC”



ROBERT KRUPA

CZŁONEK ZARZĄDU
SBM „SKARBOWIEC”

Nazwa dokumentu:	
SBM Skarbowiec	Rejestr żądań udostępnień danych osobowych
Edycja:	1
Uchwała nr	1./2021
Zastępuje:	N/D
Obowiązuje od: 05.01.2021	
Data uchwalenia: 05.01.2021	
Własność SBM Skarbowiec. Do użytku wewnętrznego. Podlega nadzorowi.	
Opracował	Zatwierdził
Katarzyna Prokopowicz	Zarząd

Odbiorca danych	Data żądania udostępnienia danych	Zakres udostępnienia danych	Data udostępnienia danych	Osoba udostępniająca dane


ROBERT KRUPA

CZŁONEK ZARZĄDU
 SBM „SKARBOWIEC”



SBM Skarbowiec	Nazwa dokumentu:		
	Procedura zarządzania ryzykiem		
	Edycja:	1	Obowiązuje od: 05.01.2021
	Uchwała nr	1/2021	Data uchwalenia: 05.01.2021
Zastępuje:	N/D		
<i>Własność SBM Skarbowiec. Do użytku wewnętrznego. Podlega nadzorowi.</i>			
Opracował		Zatwierdził	
Katarzyna Prokopowicz		Zarząd	

Cel procedury:

Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń.

Wymagania:

- 1) Analiza ryzyka przeprowadzana jest dla zbioru danych osobowych lub grupy zbiorów charakteryzujących się podobieństwem celów i sposobów przetwarzania.
- 2) Analiza ryzyka prowadzona jest w oparciu o Wytyczne Grupy Roboczej art. 29, wskazówki Urzędu Ochrony Danych Osobowych oraz inne wytyczne, które mogą stanowić wartość dodaną w procesie zarządzania ryzykiem (np. norma ISO 27001, ISO 27701).
- 3) Model procedury składa się z następujących 3 podetapów:
 - Opis systemu oparty na danych z art. 30 RODO.
 - Identyfikacja wymogów ochrony
 - Analiza ryzyka
- 4) Identyfikacja wymogów ochrony i ocena scenariuszy szkód opierają się na następujących kryteriach:
 - ocena kategorii danych zgodnie z art. 30 RODO,
 - 5-stopniowy schemat klasyfikacji wymogów ochrony który znajduje się w specyfikacji do niniejszej procedury,
 - dodatkowa analiza triady CIA → Triada CIA została opisana w specyfikacji do niniejszej procedury (C-Confidentiality), integralność (I-Integrity) i dostępność (A-Availability).




- 5) Wynik punktowy analizy ryzyka jest iloczynem sumy wartości punktowych z triady CIA oraz punktów przypisanych do 5-stopniowego schematu klasyfikacyjnego wymogów ochrony.
- 6) Po przeprowadzeniu analizy i uzyskaniu wyników należy prowadzić działania oraz wdrożyć środki ograniczające ryzyko zgodne ze specyfikacją do niniejszej procedury.
- 7) Wynikiem przeprowadzenia analizy ryzyka jest sporządzenie i prowadzenie Rejestru Czynności Przetwarzania.
- 8) Rejestr Czynności Przetwarzania prowadzony jest zgodnie z wzorem stanowiącym Załącznik 9 do Polityki Bezpieczeństwa Ochrony Danych Osobowych.
- 9) Rejestr ma formę pisemną – dopuszcza się prowadzenie rejestru w formie elektronicznej.
- 10) Rejestr jest aktualizowany w przypadku wystąpienia nowych procesów lub zajścia zmian w istniejącym procesie, jednak nie rzadziej niż raz w roku.

Specyfikacja:

5-stopniowy schemat klasyfikacyjny wymogów ochrony

poziom oceny	punkty
<p>poziom A: dane dostępne dla każdego dane osobowe są udostępniane do wglądu bez konieczności wykazywania przez osobę posiadającą taki dostęp, że zachodzi prawnie uzasadniony interes, np. dane, które właściwy organ opublikował w Internecie, w broszurach lub uzyskał z publicznie dostępnych źródeł.</p>	1
<p>poziom B: prawnie uzasadniony interes ochrony dane osobowe i poufne, których niewłaściwe wykorzystanie nie powinno spowodować żadnego konkretnego uszczerbku, ale których znajomość jest związana z prawnie uzasadnionym interesem osoby posiadającej taki dostęp, np. wewnętrzne numery telefonów, obowiązki wewnętrzne. (poziom ten nie występuje zazwyczaj w modelu czteropoziomowym.)</p>	2
<p>poziom C: podwyższony interes ochrony dane osobowe i poufne, których niewłaściwe wykorzystanie może zaszkodzić osobie, której dane dotyczą, w jej sytuacji społecznej bądź ekonomicznej (zakres: naruszenie publicznego wizerunku), np. dane dotyczące stosunków umownych, wysokości dochodu, wszelkich świadczeń socjalnych, wykroczeń).</p>	4

Cu

u

<p>poziom D: znaczny interes ochrony dane osobowe i poufne, których niewłaściwe wykorzystanie może znacznie pogorszyć sytuację społeczną lub ekonomiczną osoby, której dane dotyczą (zakres: socjalne warunki życia), np. dane dotyczące zdrowia, długi, zajęcia komornicze, niewypłacalność, przestępczość (jeżeli nie zostały sprostowane publicznie), oficjalne oceny, wyniki badań psychologiczno-medycznych.</p>	<p>8</p>
<p>poziom E: priorytetowy interes ochrony dane osobowe i poufne, których niewłaściwe wykorzystanie może zaszkodzić zdrowiu, życiu lub wolności osoby, której dane dotyczą (zakres: fizyczne warunki życia), np. adresy osób prowadzących dochodzenie pod przykryciem, dane osób, które mogą stać się potencjalnymi ofiarami przestępstwa.</p>	<p>16</p>

Kategorie wymogów ochrony

standardowy (1)	potencjalnie niewłaściwe wykorzystanie informacji poufnych wiąże się z ryzykiem finansowym dla firmy
wysoki (2)	potencjalnie niewłaściwe wykorzystanie informacji poufnych wiąże się z ryzykiem finansowym dla firmy
bardzo wysoki (3)	potencjalnie niewłaściwe wykorzystanie informacji poufnych wiąże się z krytycznymi skutkami wpływającymi na działalność firmy

kategoria danych dane osobowe ¹			atrybuty bezpieczeństwa ³			wynik ⁴
	poz. A-E ²	pkt	C	I	A	

Cm

u

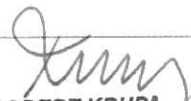
Działania i środki ograniczające ryzyko

kategoria	punkty	środki
standard	11 lub mniej	<ul style="list-style-type: none"> • Programy, aplikacje, procedury itp. mogą być instalowane na poszczególnych urządzeniach (komputer, notebook, tablet i smartphone) • Standardowe środki bezpieczeństwa są wystarczające.
wysoki	od 12 do 31	<ul style="list-style-type: none"> • Programy, aplikacje, procedury itp. mogą być instalowane na serwerach z odpowiednimi wymaganiami w zakresie ochrony (np. w ramach umowy powierzenia przetwarzania danych, aplikacji internetowych itp.) • Standardowe środki bezpieczeństwa zapewniają podstawową ochronę, ale same w sobie mogą nie być wystarczające. Należy sprawdzić zastosowanie dalszych środków w odniesieniu do przetwarzania danych. • Szczegółowy opis środków technicznych i organizacyjnych jest konieczny i musi być regularnie aktualizowany.
bardzo wysoki	32 lub więcej	<ul style="list-style-type: none"> • Programy, aplikacje, procedury itp. muszą być zainstalowane na serwerach o podwyższonych wymogach ochrony. Zwiększone wymagania w zakresie ochrony oznaczają, że przechowywanie i przetwarzanie danych odbywa się w specjalnie chronionym środowisku zgodnie z certyfikatami TÜV lub ISO. • Standardowe środki bezpieczeństwa same w sobie nie wystarczą. Należy sprawdzić dodatkowe środki bezpieczeństwa i stosować je na podstawie analizy bezpieczeństwa. • Service Level Agreements należy uzgodnić w porozumieniach umownych lub zapewnić za pomocą specjalnie dostępnych zasobów. • W przypadku połączeń komunikacyjnych między klientem a serwerem należy ustalić wiążąco odpowiednie środki ochronne dostosowane do tych zdarzeń. Należy wybrać aktualne standardy techniczne dla zapewnienia bezpiecznego łącza transmisji danych.

Wykaz zmian:

Edycja nr	Data edycji	Opis zmiany

Cu


ROBERT KRUPA
 CZŁONEK ZARZĄDU
 SBM „SKARBOWIEC”

SBM Skarbowiec	Nazwa dokumentu: Procedura nadawania i odbierania upoważnień do przetwarzania danych osobowych			
	Edycja:	1	Obowiązuje od:	05.01.2021
	Uchwała nr	1/2021	Data uchwalenia:	05.01.2021
	Zastępuje:	N/D		
<i>Własność SBM Skarbowiec. Do użytku wewnętrznego. Podlega nadzorowi.</i>				
Opracował		Zatwierdził		
Katarzyna Prokopowicz		Zarząd		

Cel procedury:

Procedura określa nadawanie i odbieranie upoważnień do przetwarzania danych osobowych. Jej celem jest uregulowanie przebiegu procesu przepływu dokumentacji oraz określenia kompetencji do udzielania i odbierania upoważnień.

Wymagania:

- 1) Każdy pracownik mający dostęp do danych osobowych musi otrzymać upoważnienie do przetwarzania danych osobowych zgodne z zajmowanym stanowiskiem przed przystąpieniem do przetwarzania danych osobowych.
- 2) Upoważnienie do przetwarzania danych osobowych odbywa się w formie pisemnej w języku zrozumiałym dla osoby upoważnianej, zgodnie z oficjalnym drukiem stanowiącym załącznik 1 do niniejszej procedury.
- 3) Upoważnienie jest nadawane przez Zarząd SBM Skarbowiec.
- 4) Zarząd SBM Skarbowiec nadaje upoważnienia do przetwarzania danych osobowych pracownikowi, z wyszczególnieniem zakresu i kategorii danych osobowych oraz systemów informatycznych, do których powinien zostać udzielony dostęp.
- 5) W przypadku konieczności zmiany zakresu upoważnienia do przetwarzania danych osobowych podległego pracownika, Zarząd zmienia upoważnienie do przetwarzania danych osobowych.
- 6) Zakres i kategoria każdego upoważnienia do przetwarzania danych osobowych jest adekwatna do zajmowanego stanowiska oraz nadawana zgodnie z zasadami

Am

u

przetwarzania danych - zgodności z prawem, rzetelności, przejrzystości, ograniczenia celu, minimalizacji danych, prawidłowości, czasowego ograniczenia przechowywania, integralności, poufności i rozliczalności (art. 5 RODO).

- 7) Każde upoważnienie jest ważne od dnia podpisania do dnia rozwiązania lub wygaśnięcia stosunku pracy, lub zmiany stanowiska pracy.

Załączniki:

Załącznik 1. Upoważnienie do przetwarzania danych osobowych

Wykaz zmian:

Edycja nr	Data edycji	Opis zmiany

MACIEJ CZYŃSKI

PREZES ZARZĄDU
SBM „SKARBOWIEC”



ROBERT KRUPA

CZŁONEK ZARZĄDU
SBM „SKARBOWIEC”

Załącznik 1. Upoważnienie do przetwarzania danych osobowych (PL)

....., dnia

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Niniejszym upoważniam Panią/Pana, zatrudnionego/zatrudnioną w SBM Skarbowiec do przetwarzania danych gromadzonych papierowo i/lub elektronicznie (zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie) zgodnie z zakresem obowiązków wynikających z zawartej umowy o pracę i/lub umowy cywilnoprawnej.
2. Niniejsze upoważnienie dotyczy: *(zaznaczyć X odpowiednie)*
 - danych osobowych zwykłych kategorii osób zatrudnionych oraz niepozostających już w zatrudnieniu, przetwarzanych w związku z ich zatrudnieniem w zakresie adekwatnym do zajmowanego stanowiska,
 - danych osobowych zwykłych kategorii dostawców oraz innych osób fizycznych, których administratorem danych jest dostawca (np. pracownicy dostawcy) przetwarzanych w związku ze współpracą z SBM Skarbowiec w zakresie adekwatnym do zajmowanego stanowiska,
 - danych osobowych zwykłych kategorii osób odwiedzających witrynę internetową SBM Skarbowiec,
 - danych osobowych zwykłych kategorii zawartych w Rejestrze Spółdzielców w zakresie adekwatnym do zajmowanego stanowiska,
 - danych osobowych zwykłych kategorii wynajmujących lokale usługowe w zakresie adekwatnym do zajmowanego stanowiska,
 - danych osobowych zwykłych kategorii członków Zarządu i Rady Nadzorczej w zakresie adekwatnym do zajmowanego stanowiska.
3. Okres trwania upoważnienia: od dnia podpisania do momentu rozwiązania lub wygaśnięcia stosunku pracy lub zmiany stanowiska pracy.
4. Podstawa prawna: art. 29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dn. 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.
5. Osoba upoważniona do przetwarzania danych objętych zakresem, o którym mowa powyżej, jest zobowiązana do zachowania ich w tajemnicy, również po ustaniu zatrudnienia, oraz zachowania w tajemnicy informacji o ich zabezpieczeniu.

.....
Podpis osoby nadającej upoważnienie
(SBM Skarbowiec)

.....
Podpis upoważnianego

.....
Podpis osoby nadającej upoważnienie
(SBM Skarbowiec)


ROBERT KRUPA
CZŁONEK ZARZĄDU
SBM „SKARBOWIEC”



SBM Skarbowiec	Nazwa dokumentu:			
	Procedura realizacji prawa do uzyskania informacji			
	Edycja:	1	Obowiązuje od:	05.01.2021
	Uchwała nr	1/2021	Data uchwalenia:	05.01.2021
Zastępuje:	N/D			
<i>Własność SBM Skarbowiec. Do użytku wewnętrznego. Podlega nadzorowi.</i>				
Opracował		Zatwierdził		
Katarzyna Prokopowicz		Zarząd		

Cel procedury:

Procedura definiuje realizację prawa do uzyskania informacji na temat Administratora Danych Osobowych zgodnie z art. 13 i 14 RODO.

Wymagania:

- 1) Każda osoba, której dane dotyczą, ma prawo uzyskania informacji na temat Administratora Danych Osobowych przed podaniem swoich danych w formie obowiązku informacyjnego.
- 2) W przypadku, w którym SBM Skarbowiec stała się Administratorem Danych Osobowych przed wysłaniem obowiązku informacyjnego należy niezwłocznie wysłać obowiązek informacyjny do osoby, której dane dotyczą.
- 3) W przypadku, w którym SBM Skarbowiec stała się Administratorem Danych Osobowych uzyskując je od osoby trzeciej, musi niezwłocznie skontaktować się z osobą, której dane dotyczą w celu spełnienia obowiązku informacyjnego, chyba, że wymagałoby to niewspółmiernego wysiłku ze strony SBM Skarbowiec w celu realizacji w/w prawa.
- 4) Informacje zawarte w obowiązku informacyjnym zostały wyszczególnione w specyfikacji do niniejszej procedury.
- 5) Obowiązki informacyjne są dopasowane do grupy odbiorców.
- 6) Każdy pracownik, przed wysłaniem obowiązku informacyjnego, jest obowiązany do przyporządkowania osoby fizycznej do właściwej grupy odbiorców oraz wysłania właściwego dokumentu.
- 7) W przypadku niemożności przyporządkowania osoby, której dane dotyczą do właściwej grupy osób, pracownik są obowiązany do skorzystania z ogólnego obowiązku informacyjnego.




8) Pracownicy nie muszą zapoznawać osoby, której dane dotyczą z obowiązkiem informacyjnym w przypadku wystąpienia przesłanek zawartych w specyfikacji do niniejszej procedury.

Specyfikacja:

Zakres informacji zawartych w obowiązku informacyjnym:

- tożsamość i dane kontaktowe Administratora (SBM Skarbowie),
- cele przetwarzania danych osobowych,
- podstawa prawna przetwarzania,
- informacja o odbiorcach danych osobowych lub o kategoriach odbiorców (jeżeli istnieją),
- informacja o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej
- okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
- informacja o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,
- informacja o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania (o ile dane zebrano na podstawie art. 6 ust 1a RODO),
- informacja o prawie wniesienia skargi do organu nadzorczego,
- informacja, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych,
- informacja o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu,
- źródło danych (w przypadku pozyskania danych osoby fizycznej od osoby trzeciej).

Am

u

Nie ma obowiązku spełnienia obowiązku informacyjnego wobec osób fizycznych, gdy:

- osoba, której dane dotyczą, dysponuje już tymi informacjami,
- udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku; w szczególności w przypadku przetwarzania do celów archiwalnych,
- pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą,
- dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy.

Załączniki:

Załącznik 1. Obowiązek informacyjny dla pracowników i zleceniobiorców

Załącznik 2. Obowiązek informacyjny dla podwykonawców

Załącznik 3. Obowiązek informacyjny dla członków spółdzielni

Załącznik 4. Obowiązek informacyjny dla osób wynajmujących lokale usługowe

Załącznik 5. Obowiązek informacyjny dla osób odwiedzających stronę www (Polityka Prywatności)

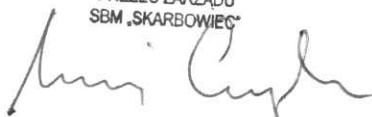
Załącznik 6. Obowiązek informacyjny dla Członków Zarządu i Rady Nadzorczej

Wykaz zmian:

Edycja nr	Data edycji	Opis zmiany

MACIEJ CZYŃSKI

PREZES ZARZĄDU
SBM „SKARBOWIEC”



ROBERT KRUPA

CZŁONEK ZARZĄDU
SBM „SKARBOWIEC”

Załącznik 1. Obowiązek informacyjny dla pracowników i zleceniobiorców

1. Administratorem Pani/Pana danych osobowych jest Spółdzielnia Budowlano-Mieszkaniowa „Skarbowiec”, ul. Grójecka 41, 02-031 Warszawa
2. Inspektorem Ochrony Danych jest Katarzyna Prokopowicz. Z IOD można skontaktować się pod numerem telefonu 600 004 503, mailowo: iod@skarbowiec.waw.pl lub listownie pod adresem Spółdzielni.
3. Pani/Pana dane osobowe będą przetwarzane w celu: wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy lub do wypełnienia prawnie usprawiedliwionych celów realizowanych przez SBM Skarbowiec.
4. Podane dane zwykłych kategorii będą przetwarzane na podstawie art. 6 ust. 1 lit. b, c lub f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016. Podane dane szczególnych kategorii będą przetwarzane na podstawie art. 9 ust. 2 lit. b lub c Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016.
5. Podanie danych jest dobrowolne, aczkolwiek konieczne do realizacji celów, w jakich są zbierane.
6. Dane będą udostępniane podmiotom zewnętrznym w przypadkach przewidzianych przepisami prawa, a na podstawie umów powierzenia będą przekazywane podmiotom świadczącym usługi na rzecz SBM Skarbowiec, takimi jak: dostawcy usług zewnętrznych, dostawcy systemów informatycznych oraz inni podwykonawcy.
7. Dane przechowywane będą przez okres niezbędny do wykonania postanowień umowy oraz czas niezbędny ze względu na obowiązki wynikające z regulacji księgowych i podatkowych lub innych przepisów prawa.
8. Ma Pani/Pan prawo dostępu do treści swoich danych oraz z zastrzeżeniem przepisów prawa: prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo do wniesienia sprzeciwu.
9. Ma Pani/Pan prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
10. Dane mogą zostać przekazane do państw trzecich na mocy Standardowych Klauzul Umownych. Pani/Pana dane nie będą przetwarzane w sposób zautomatyzowany i nie będą poddawane profilowaniu.

MACIEJ CZYŃSKI

PREZES ZARZĄDU
SBM „SKARBOWIEC”



ROBERT KRUPA

CZŁONEK ZARZĄDU
SBM „SKARBOWIEC”

Załącznik 2. Obowiązek informacyjny dla podwykonawców

1. Administratorem Pani/Pana danych osobowych jest Spółdzielnia Budowlano-Mieszkaniowa „Skarbowiec”, ul. Grójecka 41, 02-031 Warszawa
2. Inspektorem Ochrony Danych jest Katarzyna Prokopowicz. Z IOD można skontaktować się pod numerem telefonu 600 004 503, mailowo: iod@skarbowiec.waw.pl lub listownie pod adresem Spółdzielni.
3. Pani/Pana dane osobowe będą przetwarzane w celu: wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy lub do wypełnienia prawnie usprawiedliwionych celów realizowanych przez SBM Skarbowiec.
4. Podane dane zwykłych kategorii będą przetwarzane na podstawie art. 6 ust. 1 lit. b, c lub f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016.
5. Podanie danych jest dobrowolne, aczkolwiek konieczne do realizacji celów, w jakich są zbierane.
6. Dane będą udostępniane podmiotom zewnętrznym w przypadkach przewidzianych przepisami prawa, a na podstawie umów powierzenia będą przekazywane podmiotom świadczącym usługi na rzecz SBM Skarbowiec, takimi jak: dostawcy usług zewnętrznych, dostawcy systemów informatycznych oraz inni podwykonawcy.
7. Dane przechowywane będą przez okres niezbędny do wykonania postanowień umowy oraz czas niezbędny ze względu na obowiązki wynikające z regulacji księgowych i podatkowych lub innych przepisów prawa.
8. Ma Pani/Pan prawo dostępu do treści swoich danych oraz z zastrzeżeniem przepisów prawa: prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo do wniesienia sprzeciwu.
9. Ma Pani/Pan prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
10. Dane mogą zostać przekazane do państw trzecich na mocy Standardowych Klauzul Umownych. Pani/Pana dane nie będą przetwarzane w sposób zautomatyzowany i nie będą poddawane profilowaniu.

MACIEJ CZYŃSKI

PREZES ZARZĄDU
SBM „SKARBOWIEC”



ROBERT KRUPA

CZŁONEK ZARZĄDU
SBM „SKARBOWIEC”

Załącznik 3. Obowiązek informacyjny dla Członków Spółdzielni

1. Administratorem Pani/Pana danych osobowych jest Spółdzielnia Budowlano-Mieszkaniowa „Skarbowiec”, ul. Grójecka 41, 02-031 Warszawa
2. Inspektorem Ochrony Danych jest Katarzyna Prokopowicz. Z IOD można skontaktować się pod numerem telefonu 600 004 503, mailowo: iod@skarbowiec.waw.pl lub listownie pod adresem Spółdzielni.
3. Pani/Pana dane osobowe będą przetwarzane w celu: wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy, wypełniania obowiązków prawnych lub do wypełnienia prawnie usprawiedliwionych celów realizowanych przez SBM Skarbowiec.
4. Podane dane zwykłych kategorii będą przetwarzane na podstawie art. 6 ust. 1 lit. b, c lub f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016.
5. Podanie danych jest dobrowolne, aczkolwiek konieczne do realizacji celów, w jakich są zbierane.
6. Dane będą udostępniane podmiotom zewnętrznym w przypadkach przewidzianych przepisami prawa, a na podstawie umów powierzenia będą przekazywane podmiotom świadczącym usługi na rzecz SBM Skarbowiec, takimi jak: dostawcy usług zewnętrznych, dostawcy systemów informatycznych oraz inni podwykonawcy.
7. Dane przechowywane będą przez okres niezbędny do wykonania postanowień umowy oraz czas niezbędny ze względu na obowiązki wynikające z regulacji księgowych i podatkowych lub innych przepisów prawa.
8. Ma Pani/Pan prawo dostępu do treści swoich danych oraz z zastrzeżeniem przepisów prawa: prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo do wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie.
9. Ma Pani/Pan prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
10. Dane mogą zostać przekazane do państw trzecich na mocy Standardowych Klauzul Umownych. Pani/Pana dane nie będą przetwarzane w sposób zautomatyzowany i nie będą poddawane profilowaniu.

MACIEJ CZYŃSKI

PREZES ZARZĄDU
SBM „SKARBOWIEC”



ROBERT KRUPA

CZŁONEK ZARZĄDU
SBM „SKARBOWIEC”

Załącznik 4. Obowiązek informacyjny dla osób wynajmujących lokale usługowe

1. Administratorem Pani/Pana danych osobowych jest Spółdzielnia Budowlano-Mieszkaniowa „Skarbowiec”, ul. Grójecka 41, 02-031 Warszawa
2. Inspektorem Ochrony Danych jest Katarzyna Prokopowicz. Z IOD można skontaktować się pod numerem telefonu 600 004 503, mailowo: iod@skarbowiec.waw.pl lub listownie pod adresem Spółdzielni.
3. Pani/Pana dane osobowe będą przetwarzane w celu: wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy, wypełniania obowiązków prawnych lub do wypełnienia prawnie usprawiedliwionych celów realizowanych przez SBM Skarbowiec.
4. Podane dane zwykłych kategorii będą przetwarzane na podstawie art. 6 ust. 1 lit. b, c lub f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016.
5. Podanie danych jest dobrowolne, aczkolwiek konieczne do realizacji celów, w jakich są zbierane.
6. Dane będą udostępniane podmiotom zewnętrznym w przypadkach przewidzianych przepisami prawa, a na podstawie umów powierzenia będą przekazywane podmiotom świadczącym usługi na rzecz SBM Skarbowiec, takimi jak: dostawcy usług zewnętrznych, dostawcy systemów informatycznych oraz inni podwykonawcy.
7. Dane przechowywane będą przez okres niezbędny do wykonania postanowień umowy oraz czas niezbędny ze względu na obowiązki wynikające z regulacji księgowych i podatkowych lub innych przepisów prawa.
8. Ma Pani/Pan prawo dostępu do treści swoich danych oraz z zastrzeżeniem przepisów prawa: prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo do wniesienia sprzeciwu.
9. Ma Pani/Pan prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
10. Dane mogą zostać przekazane do państw trzecich na mocy Standardowych Klauzul Umownych. Pani/Pana dane nie będą przetwarzane w sposób zautomatyzowany i nie będą poddawane profilowaniu.

MACIEJ CZYŃSKI

PREZES ZARZĄDU
SBM „SKARBOWIEC”




ROBERT KRUPA

CZŁONEK ZARZĄDU
SBM „SKARBOWIEC”

Załącznik 5. Obowiązek informacyjny dla osób odwiedzających stronę www (Polityka Prywatności)

Zgodnie z art. 13 ust 1 i 2 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. prosimy o zapoznanie się z poniższymi zagadnieniami.

Kto jest administratorem Twoich danych osobowych?

Administratorem Twoich danych osobowych jest Spółdzielnia Budowlano-Mieszkaniowa „Skarbowiec”, ul. Grójecka 41, 02-031 Warszawa.

Inspektor Ochrony Danych

Funkcję Inspektora Ochrony Danych Katarzyna Prokopowicz. Z IOD można skontaktować się pod numerem telefonu 600 004 503, mailowo: iod@skarbowiec.waw.pl lub listownie pod adresem Spółdzielni.

W jakich celach i na jakiej podstawie przechowujemy Twoje dane?

Twoje dane osobowe przetwarzamy w następujących celach:

- zawarcia i wykonania łączącej nas umowy (art. 6 ust. 1 b RODO – wykonanie umowy);
- kontaktu w sprawie łączącej nas umowy (art. 6 ust. 1 b RODO – wykonanie umowy);
- obsługi Twoich zapytań i skarg, w tym rozwiązywania problemów (art. 6 ust. 1 c RODO – wykonanie ciążących na nas obowiązków prawnych);
- dokonywania rozliczeń (art. 6 ust. 1 c RODO – wykonanie ciążących na nas obowiązków prawnych);
- analiz i badań sposobu korzystania przez Ciebie witryny internetowej (art. 6 ust. 1 f RODO – nasz uzasadniony interes);
- prowadzenia postępowań sądowych i administracyjnych (art. 6 ust. 1 f RODO – nasz prawnie uzasadniony interes);
- w celach marketingowych (w trakcie łączącej nas umowy: art. 6 ust. 1 f RODO – nasz uzasadniony interes, po zakończeniu łączącej nas umowy: art. 6 ust. 1 a RODO – wyrażenie zgody).

Jakie dane zbieramy?

MACIEJ CZYŃSKI

PREZES ZARZĄDU
SBM „SKARBOWIEC”



ROBERT KRUPA

CZŁONEK ZARZĄDU
SBM „SKARBOWIEC”

Automatyczne podejmowanie decyzji

Twoje dane nie będą przetwarzane w sposób zautomatyzowany, w tym również w formie profilowania.

Załącznik 6. Obowiązek informacyjny dla Członków Zarządu i Rady Nadzorczej

1. Administratorem Pani/Pana danych osobowych jest Spółdzielnia Budowlano-Mieszkaniowa „Skarbowiec”, ul. Grójecka 41, 02-031 Warszawa
2. Inspektorem Ochrony Danych jest Katarzyna Prokopowicz. Z IOD można skontaktować się pod numerem telefonu 600 004 503, mailowo: iod@skarbowiec.waw.pl lub listownie pod adresem Spółdzielni.
3. Pani/Pana dane osobowe będą przetwarzane w celu: wykonania umowy, której stroną jest osoba, której dane dotyczą lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy lub do wypełnienia innych obowiązków prawnych.
4. Podane dane zwykłych kategorii będą przetwarzane na podstawie art. 6 ust. 1 lit. b lub c Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016.
5. Podanie danych jest dobrowolne, aczkolwiek konieczne do realizacji celów, w jakich są zbierane.
6. Dane będą udostępniane podmiotom zewnętrznym w przypadkach przewidzianych przepisami prawa, a na podstawie umów powierzenia będą przekazywane podmiotom świadczącym usługi na rzecz SBM Skarbowiec, takimi jak: dostawcy usług zewnętrznych, dostawcy systemów informatycznych oraz inni podwykonawcy.
7. Dane przechowywane będą przez okres niezbędny do wykonania postanowień umowy oraz czas niezbędny ze względu na obowiązki wynikające z regulacji księgowych i podatkowych lub innych przepisów prawa.
8. Ma Pani/Pan prawo dostępu do treści swoich danych oraz z zastrzeżeniem przepisów prawa: prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo do wniesienia sprzeciwu.
9. Ma Pani/Pan prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
10. Dane mogą zostać przekazane do państw trzecich na mocy Standardowych Klauzul Umownych. Pani/Pana dane nie będą przetwarzane w sposób zautomatyzowany i nie będą poddawane profilowaniu.



ROBERT KRUPA

CZŁONEK ZARZĄDU
SBM „SKARBOWIEC”



Zbieramy dane, które są niezbędne do wykonania usługi kierując się zasadą minimalizacji. Jeżeli prosimy Cię o podanie danych to dlatego, że są nam one niezbędne do realizacji celu. Jeżeli chcesz otrzymywać od nas biuletyny wysyłane w formie elektronicznej to poprosimy Cię również o podanie swojego adresu mailowego.

Komu przekazujemy Twoje dane?

Twoje dane przekazujemy:

1. Podmiotom przetwarzającym, tj. firmom, z którymi współpracujemy i które przetwarzają dane na nasze żądanie.
2. Innym administratorom danych przetwarzającym Twoje dane we własnym imieniu, m.in. firmom pocztowym itp. podmiotom współpracującym.

Twoje dane osobowe mogą zostać przekazane do państwa trzeciego na mocy standardowych klauzul umownych.

Ile czasu przechowujemy Twoje dane?

Twoje dane przechowywane będą przez okres niezbędny do wykonania postanowień umowy oraz czas niezbędny ze względu na obowiązki wynikające z regulacji księgowych i podatkowych lub innych przepisów prawa.

Jakie masz prawa?

Masz prawo do dostępu do treści swoich danych, sprostowania danych, usunięcia danych, ograniczenia przetwarzania danych, przenoszenia danych, wniesienia sprzeciwu, cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.

Masz również prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych w momencie, w którym uznasz, iż przetwarzanie Twoich danych osobowych dotyczących narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27.04.2016 r.

Czy musisz podawać dane?

Podanie powyższych danych jest dobrowolne, aczkolwiek konieczne w przypadku, kiedy chcesz skorzystać z naszych usług. Podanie niektórych danych jest wymogiem ustawowym. Przed podaniem swoich danych zostaniesz o tym poinformowany.

SBM Skarbowiec	Nazwa dokumentu:			
	Procedura realizacji prawa dostępu do danych osobowych			
	Edycja:	1	Obowiązuje od:	05.01.2021
	Uchwała nr	1/2021	Data uchwalenia:	05.01.2021
Zastępuje:	N/D			
<i>Własność SBM Skarbowiec. Do użytku wewnętrznego. Podlega nadzorowi.</i>				
Opracował		Zatwierdził		
Katarzyna Prokopowicz		Zarząd		

Cel procedury:

Procedura definiuje realizację prawa dostępu do danych w związanej, przejrzystej, zrozumiałej i łatwo dostępnej formie, przekazanej jasnym i prostym językiem (art. 12 ust. 1 RODO) zgodnie z art. 15 RODO.

Wymagania:

- 1) Każda osoba fizyczna, której dane dotyczą, ma prawo zwrócić się do SBM Skarbowiec w celu uzyskania dostępu do swoich danych.
- 2) Żądania osób fizycznych w zakresie realizacji prawa dostępu do danych może być kierowane:
 - a. drogą pisemną na adres: SBM Skarbowiec, ul. Grójecka 41, 02-031 Warszawa
 - b. drogą mailową na adres: iod@skarbowiec.waw.pl
- 3) Administrator Danych Osobowych ma obowiązek zweryfikować osobę fizyczną, której dane dotyczą zgodnie z zakresem danych zawartym w specyfikacji niniejszej procedury.
- 4) Administrator Danych Osobowych wydaje polecenie dokonania sprawdzenia posiadania danych osoby, której dane dotyczą w sieci IT.
- 5) Administrator Danych Osobowych wydaje polecenie dokonania sprawdzenia posiadania danych osoby, której dane dotyczą w swoich zasobach, w tym na nagraniach z monitoringu (w przypadku posiadania statusu Administratora Danych Osobowych).
- 6) Wszyscy pracownicy, do których zwróci Administrator Danych Osobowych odpowiadają na żądanie Administratora niezwłocznie, jednak w terminie nie dłuższym niż 14 dni.
- 7) W przypadku osób fizycznych, których dane SBM Skarbowiec przetwarza – prawo dostępu do danych realizowane jest poprzez przekazanie żądanych informacji na piśmie lub drogą elektroniczną zgodnie z żądaniem osoby, której dane dotyczą.

lu

lu

- 8) W przypadku przekazywania informacji drogą elektroniczną Administrator zapewni, że przesyłane dane będą zabezpieczone w odpowiedni sposób zapewniający bezpieczeństwo.
- 9) Administrator Danych Osobowych odnosi się do żądania osoby fizycznej w terminie nie dłuższym niż 30 dni.
- 10) W przypadku, w którym realizacja prawa dostępu do danych nie mogła zostać zrealizowana w terminie, Administrator wysła osobie fizycznej, której dane dotyczą informację o przyczynach przedłużenia procesu.
- 11) Pierwsza kopia danych jest wydawana przez Administratora nieodpłatnie, natomiast za każdą kolejną kopię danych osobowych Administrator może pobrać opłatę w wysokości wynikającej z kosztów administracyjnych.
- 12) Administrator zapewnia, że podczas obsługi realizacji praw związanych z dostępem do danych, nie narusza praw innych osób, w tym tajemnic handlowych, własności intelektualnej oraz praw autorskich chroniących oprogramowanie.

Specyfikacja:

Dane do weryfikacji osoby, której dane dotyczą:

- imię, nazwisko, której zgłoszenie dotyczy oraz osoby zgłaszającej,
- opis zgłaszanego żądania wraz ze wskazaniem ewentualnych zastrzeżeń,
- podpis osoby zgłaszającej żądanie w przypadku zgłoszeń pisemnych,
- pełnomocnictwo, jeśli w imieniu zgłaszającego żądanie działa pełnomocnik,
- informacje o preferowanej formie odpowiedzi, jeżeli kanał odpowiedzi ma być inny niż zgłoszone żądanie.

W przypadku braku możliwości identyfikacji wnioskodawcy lub zaistnienia wątpliwości co do jego tożsamości, w celu zachowania bezpieczeństwa przetwarzanych danych osobowych, Administrator Danych Osobowych może zażądać dodatkowych danych potwierdzających tożsamość wnoszącego.

Wykaz zmian:

Edycja nr	Data edycji	Opis zmiany

MACIEJ CZYŃSKI

PREZES ZARZĄDU
SBM „SKARBOWIEC”

ROBERT KRUPA

CZŁONEK ZARZĄDU
SBM „SKARBOWIEC”

SBM Skarbowiec	Nazwa dokumentu:			
	Procedura realizacji prawa do sprostowania danych			
	Edycja:	1	Obowiązuje od:	05.01.2021
	Uchwała nr	1/2021	Data uchwalenia:	05.01.2021
Zastępuje:	N/D			
<i>Własność SBM Skarbowiec. Do użytku wewnętrznego. Podlega nadzorowi.</i>				
Opracował		Zatwierdził		
Katarzyna Prokopowicz		Zarząd		

Cel procedury:

Procedura definiuje realizację prawa do poprawiania danych osobowych zgodnie z art. 16 RODO.

Wymagania:

- 1) Każda osoba, której dane dotyczą, ma prawo żądania od SBM Skarbowiec niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe.
- 2) Osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.
- 3) Żądania osób fizycznych w zakresie realizacji prawa do sprostowania danych może być kierowane:
 - a. drogą pisemną na adres: SBM Skarbowiec, ul. Grójecka 41, 02-031 Warszawa
 - b. drogą mailową na adres: iod@skarbowiec.waw.pl
- 4) Administrator Danych Osobowych ma obowiązek zweryfikować osobę fizyczną, której dane dotyczą zgodnie z zakresem danych zawartym w specyfikacji niniejszej procedury.
- 5) Administrator Danych Osobowych wydaje polecenie aktualizacji w sieci IT danych osoby, której dane dotyczą, w tym również w zarchiwizowanych kopiach, chyba, że wymagałoby to niewspółmiernie dużego wysiłku.
- 6) Administrator Danych Osobowych wydaje polecenie dokonania sprawdzenia posiadania danych osoby, której dane dotyczą w swoich zasobach.
- 7) Wszyscy pracownicy, do których zwróci się Administrator Danych Osobowych odpowiadają na żądanie Administratora niezwłocznie, jednak w terminie nie dłuższym niż 7 dni.

- 8) W przypadku osób fizycznych, których dane Administrator przetwarza – prawo do sprostowania danych realizowane jest poprzez wykonanie żądania osoby, której dane dotyczą i przekazanie informacji zwrotnej na piśmie lub drogą elektroniczną osobie fizycznej, zgodnie z jej żądaniem.
- 9) W przypadku przekazywania informacji drogą elektroniczną Administrator zapewni, że przesyłane dane będą zabezpieczone w odpowiedni sposób zapewniający bezpieczeństwo.
- 10) Administrator odnosi się do żądania osoby fizycznej w terminie nie dłuższym niż 14 dni.
- 11) W przypadku, w którym realizacja prawa do sprostowania danych nie mogła zostać zrealizowana w terminie, Administrator wysyła osobie fizycznej, której dane dotyczą informację o przyczynach przedłużenia procesu.
- 12) Administrator zapewnia, że podczas obsługi realizacji praw związanych z prawem do sprostowania danych, nie narusza praw innych osób, w tym tajemnic handlowych, własności intelektualnej oraz praw autorskich chroniących oprogramowanie.

Specyfikacja:

Minimalny zakres danych niezbędnych do weryfikacji osoby, której dane dotyczą:

- imię, nazwisko, której zgłoszenie dotyczy oraz osoby zgłaszającej,
- wskazanie niepoprawnych i/lub nieaktualnych danych,
- wskazanie poprawnych i/lub aktualnych danych,
- podpis osoby zgłaszającej żądanie w przypadku zgłoszeń pisemnych,
- pełnomocnictwo, jeśli w imieniu zgłaszającego żądanie działa pełnomocnik,
- informacje o preferowanej formie odpowiedzi, jeżeli kanał odpowiedzi ma być inny niż zgłoszone żądanie.

W przypadku braku możliwości identyfikacji wnioskodawcy lub zaistnienia wątpliwości co do jego tożsamości, w celu zachowania bezpieczeństwa przetwarzanych danych osobowych, Administrator może zażądać dodatkowych danych potwierdzających tożsamość wnoszącego.

Wykaz zmian:

Edycja nr	Data edycji	Opis zmiany

MACIEJ CZYŃSKI

 PREZES ZARZĄDU
 SBM „SKARBOWIEC”


ROBERT KRUPA
 CZŁONEK ZARZĄDU
 SBM „SKARBOWIEC”

SBM Skarbowiec	Nazwa dokumentu:			
	Procedura realizacji prawa do usunięcia danych			
	Edycja:	1	Obowiązuje od:	05.01.2021
	Uchwała nr	1/2021	Data uchwalenia:	05.01.2021
Zastępuje:	N/D			
<i>Własność SBM Skarbowiec. Do użytku wewnętrznego. Podlega nadzorowi.</i>				
Opracował		Zatwierdził		
Katarzyna Prokopowicz		Zarząd		

Cel procedury:

Procedura definiuje realizację prawa do usunięcia danych osobowych zgodnie z art. 17 RODO.

Wymagania:

- 1) Każda osoba, której dane dotyczą ma prawo żądania od SBM Skarbowiec niezwłocznego usunięcia danych lub skorzystania z prawa do bycia zapomnianych, w przypadkach opisanych w specyfikacji niniejszej procedury.
- 2) Osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.
- 3) Żądania osób fizycznych w zakresie realizacji prawa do usunięcia danych może być kierowane:
 - a. drogą pisemną na adres: SBM Skarbowiec, ul. Grójecka 41, 02-031 Warszawa
 - b. drogą mailową na adres: iod@skarbowiec.waw.pl
- 4) Administrator Danych Osobowych ma obowiązek zweryfikować osobę fizyczną, której dane dotyczą zgodnie z zakresem danych zawartym w specyfikacji niniejszej procedury.
- 5) Administrator Danych Osobowych wydaje polecenie aktualizacji w sieci IT danych osoby, której dane dotyczą, w tym również w zarchiwizowanych kopiach, chyba, że wymagałoby to niewspółmiernie dużego wysiłku.
- 6) Administrator Danych Osobowych wydaje polecenie dokonania sprawdzenia posiadania danych osoby, której dane dotyczą w swoich zasobach.
- 7) Wszyscy pracownicy, do których zwróci się Administrator Danych Osobowych odpowiadają na żądanie Koordynatora niezwłocznie, jednak w terminie nie dłuższym niż 7 dni.
- 8) W przypadku osób fizycznych, których dane Administrator przetwarza – prawo do usunięcia danych realizowane jest poprzez wykonanie żądania osoby, której dane dot.

Ar

SBM SKARBOWIEC

u

- 9) Administrator odnosi się do żądania osoby fizycznej w terminie nie dłuższym niż 14 dni.
- 10) W przypadku, w którym realizacja prawa do sprostowania danych nie mogła zostać zrealizowana w terminie, Koordynator wysyła osobie fizycznej, której dane dotyczą informację o przyczynach przedłużenia procesu.
- 11) Administrator zapewnia, że podczas obsługi realizacji praw związanych z prawem do usunięcia danych, nie narusza praw innych osób, w tym tajemnic handlowych, własności intelektualnej oraz praw autorskich chroniących oprogramowanie.

Specyfikacja:

Minimalny zakres danych niezbędnych do weryfikacji osoby, której dane dotyczą:

- imię, nazwisko osoby której zgłoszenie dotyczy oraz osoby zgłaszającej,
- wskazanie żądania wraz ze wskazaniem ewentualnych zastrzeżeń,
- podpis osoby zgłaszającej żądanie w przypadku zgłoszeń pisemnych,
- pełnomocnictwo, jeśli w imieniu zgłaszającego żądanie działa pełnomocnik.

W przypadku braku możliwości identyfikacji wnioskodawcy lub zaistnienia wątpliwości co do jego tożsamości, w celu zachowania bezpieczeństwa przetwarzanych danych osobowych, Koordynator Danych Osobowych może zażądać dodatkowych danych potwierdzających tożsamość wnoszącego.

Osoba, której dane dotyczą ma prawo żądać usunięcia danych jeżeli:

- dane są niekompletne, nieaktualne, nieprawdziwe,
- dane nie są już niezbędne do realizacji celu, w którym zostały zebrane,
- cofnęła ona zgodę, na podstawie której opierało się przetwarzanie i nie ma innej podstawy do tego, aby dane te dalej przetwarzać,
- wniosła sprzeciw wobec przetwarzania prowadzonego na potrzeby marketingu bezpośredniego, przetwarzania, które jest niezbędne do wykonania zadania realizowanego

Osoba, której dane dotyczą może skorzystać z prawa do bycia zapomnianym w przypadku:

- upublicznienia danych przez Administratora.

Wykaz zmian:

Edycja nr	Data edycji	Opis zmiany

MACIEJ CZYŃSKI
 PREZES ZARZĄDU
 SBM „SKARBOWIEC”


ROBERT KRUPA
 CZŁONEK ZARZĄDU
 SBM „SKARBOWIEC”

SBM Skarbowiec	Nazwa dokumentu:			
	Procedura realizacji prawa do ograniczenia przetwarzania danych osobowych			
	Edycja:	1	Obowiązuje od:	05.01.2021
	Uchwała nr	1/2021	Data uchwalenia:	05.01.2021
	Zastępuje:	N/D		
<i>Własność SBM Skarbowiec. Do użytku wewnętrznego. Podlega nadzorowi.</i>				
Opracował		Zatwierdził		
Katarzyna Prokopowicz		Zarząd		

Cel procedury:

Procedura definiuje realizację prawa do ograniczenia przetwarzania danych osobowych

Wymagania:

- 1) Osoba fizyczna, której dane dotyczą, ma prawo żądać ograniczenia przetwarzania w następujących przypadkach:
 - a. osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający Administratorowi sprawdzić prawidłowość tych danych,
 - b. przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
 - c. Administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,
 - d. osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie Administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.
- 2) Pracownik, do którego zwróciła się osoba fizyczna, której dane dotyczą jest obowiązany niezwłocznie powiadomić Administratora Danych Osobowych, jednak w terminie nie dłuższym niż 3 dni.




- 3) Administrator Danych Osobowych ma obowiązek zweryfikować osobę fizyczną, której dane dotyczą zgodnie z zakresem danych zawartym w specyfikacji niniejszej procedury.
- 4) W przypadku uwzględnienia żądania ograniczenia przetwarzania Administrator Danych Osobowych zleca zabezpieczenie danych, w taki sposób, że użytkownicy systemu nie będą mieli do tych danych dostępu, oraz że nie będą podlegały dalszemu przetwarzaniu ani modyfikacjom.
- 5) W przypadku ograniczenia przetwarzania dane osobowe będą przetwarzane wyłącznie w zakresie ich przechowywania. Przetwarzanie danych w innym celu jest wyłącznie możliwe:
 - a. gdy osoba fizyczna wyrazi zgodę na inny cel przetwarzania,
 - b. w celu ustalenia, dochodzenia lub obrony roszczeń,
 - c. w celu ochrony praw innej osoby fizycznej lub prawnej,
 - d. z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego.
- 6) Administrator Danych Osobowych przekazuje informację zwrotną osobie, której dane dotyczą w preferowanej przez osobę fizyczną formie.
- 7) Administrator zapewnia, że podczas obsługi realizacji praw związanych z ograniczeniem celu przetwarzania danych, nie narusza praw innych osób, w tym tajemnic handlowych, własności intelektualnej oraz praw autorskich chroniących oprogramowanie.

Specyfikacja:

Żądania osób fizycznych w zakresie realizacji prawa do ograniczenia przetwarzania danych osobowych może być kierowane:

- a. drogą pisemną na adres: SBM Skarbowiec, ul. Grójecka 41, 02-031 Warszawa
- b. drogą mailową na adres: iod@skarbowiec.waw.pl

Dane do weryfikacji osoby, której dane dotyczą:

- imię, nazwisko, której zgłoszenie dotyczy oraz osoby zgłaszającej,
- opis zgłaszanego żądania wraz ze wskazaniem ewentualnych zastrzeżeń,
- podpis osoby zgłaszającej żądanie w przypadku zgłoszeń pisemnych,
- pełnomocnictwo, jeśli w imieniu zgłaszającego żądanie działa pełnomocnik,



- informacje o preferowanej formie odpowiedzi, jeżeli kanał odpowiedzi ma być inny niż zgłoszone żądanie.

W przypadku braku możliwości identyfikacji wnioskodawcy lub zaistnienia wątpliwości co do jego tożsamości, w celu zachowania bezpieczeństwa przetwarzanych danych osobowych, Administrator może zażądać dodatkowych danych potwierdzających tożsamość wnoszącego.

Wykaz zmian:

Edycja nr	Data edycji	Opis zmiany

MACIEJ CZYŃSKI
PREZES ZARZĄDU
SBM „SKARBOWIEC”



ROBERT KRUPA
CZŁONEK ZARZĄDU
SBM „SKARBOWIEC”

SBM Skarbowiec	Nazwa dokumentu:			
	Procedura realizacji prawa do przenoszenia danych			
	Edycja:	1	Obowiązuje od:	05.01.2021
	Uchwała nr	1/2021	Data uchwalenia:	05.01.2021
Zastępuje:	N/D			
<i>Własność SBM Skarbowiec. Do użytku wewnętrznego. Podlega nadzorowi.</i>				
Opracował		Zatwierdził		
Katarzyna Prokopowicz		Zarząd		

Cel procedury:

Procedura definiuje realizację prawa do przenoszenia danych osobowych zgodnie z art. 20 RODO.

Wymagania:

- 1) Prawo do przenoszenia danych obejmuje:
 - a. prawo do otrzymania danych od Administratora,
 - b. prawo do przesłania danych bez utrudnień ze strony Administratora,
 - c. prawo do przesłania danych bezpośrednio pomiędzy administratorami, bez pośrednictwa osoby, której dane dotyczą (o ile jest to technicznie możliwe).
- 2) Prawo do przenoszenia danych przysługuje jedynie w przypadku, gdy przetwarzanie danych odbywa się na podstawie zgody osoby fizycznej lub umowy (w myśl art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a lub na podstawie umowy w myśl art. 6 ust. 1 lit. b) **oraz** w sposób zautomatyzowany.
- 3) Żądania osób fizycznych w zakresie realizacji prawa do przenoszenia danych może być kierowane:
 - a. drogą pisemną na adres: SBM Skarbowiec, ul. Grójecka 41, 02-031 Warszawa
 - b. drogą mailową na adres: iod@skarbowiec.waw.pl
- 4) Administrator Danych Osobowych ma obowiązek zweryfikować osobę fizyczną, której dane dotyczą zgodnie z zakresem danych zawartym w specyfikacji niniejszej procedury.

[Handwritten signature]

[Faint stamp]

[Handwritten mark]

- 5) W przypadku uwzględnienia wniosku dot. przeniesienia danych, dane zostaną udostępnione w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego.
- 6) W przypadku przekazywania informacji drogą elektroniczną Administrator Danych Osobowych zapewni, że przesyłane dane będą zabezpieczone w odpowiedni sposób zapewniający bezpieczeństwo.
- 7) Administrator odnosi się do żądania osoby fizycznej w terminie nie dłuższym niż 14 dni.
- 8) W przypadku, w którym realizacja prawa do sprostowania danych nie mogła zostać zrealizowana w terminie, Administrator wysłał osobie fizycznej, której dane dotyczą informację o przyczynach przedłużenia procesu.
- 9) Administrator zapewnia, że podczas obsługi realizacji praw związanych z prawem do przenoszenia danych, nie narusza praw innych osób, w tym tajemnic handlowych, własności intelektualnej oraz praw autorskich chroniących oprogramowanie.

Specyfikacja:

Minimalny zakres danych niezbędnych do weryfikacji osoby, której dane dotyczą:

- imię, nazwisko, której zgłoszenie dotyczy oraz osoby zgłaszającej,
- opis zgłaszanego żądania wraz ze wskazaniem ewentualnych zastrzeżeń,
- podpis osoby zgłaszającej żądanie w przypadku zgłoszeń pisemnych,
- pełnomocnictwo, jeśli w imieniu zgłaszającego żądanie działa pełnomocnik,
- informacje o preferowanej formie odpowiedzi, jeżeli kanał odpowiedzi ma być inny niż zgłoszone żądanie.

W przypadku braku możliwości identyfikacji wnioskodawcy lub zaistnienia wątpliwości co do jego tożsamości, w celu zachowania bezpieczeństwa przetwarzanych danych osobowych, Administrator może zażądać dodatkowych danych potwierdzających tożsamość wnoszącego.

Wykaz zmian:

Edycja nr	Data edycji	Opis zmiany

MACIEJ CZYŃSKI
 PREZES ZARZĄDU
 SBM „SKARBOWIEC”

ROBERT KRUPA
 CZŁONEK ZARZĄDU
 SBM „SKARBOWIEC”

SBM Skarbowiec	Nazwa dokumentu:			
	Procedura realizacji prawa do sprzeciwu			
	Edycja:	1	Obowiązuje od:	05.01.2021
	Uchwała nr	1/2021	Data uchwalenia:	05.01.2021
Zastępuje:	N/D			
<i>Własność SBM Skarbowiec. Do użytku wewnętrznego. Podlega nadzorowi.</i>				
Opracował		Zatwierdził		
Katarzyna Prokopowicz		Zarząd		

Cel procedury:

Procedura definiuje realizację prawa do sprzeciwu zgodnie z art. 21 RODO.

Wymagania:

- 1) Osoba fizyczna ma prawo do sprzeciwu wobec przetwarzania danych osobowych, gdy Administrator przetwarza dane na podstawie przesłanki prawnie uzasadnionego interesu (art. 6 ust. 1 lit. f RODO) w tym profilowania.
- 2) Administrator może odmówić zaprzestania przetwarzania danych osobowych, powołując się na:
 - a. istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania danych, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą,
 - b. istnienie podstaw do ustalenia, dochodzenia lub obrony roszczeń.
- 3) W przypadku zgłoszenia sprzeciwu wobec przetwarzania danych w celach marketingu bezpośredniego, w tym profilowania w zakresie w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim, żądanie osoby fizycznej podlega niezwłocznemu i bezwarunkowemu uwzględnieniu. Administrator zapewni, że dane osobowe nie będą już przetwarzane w tym w tym celu.
- 4) Żądania osób fizycznych w zakresie realizacji prawa do sprzeciwu może być kierowane:
 - a. drogą pisemną na adres: SBM Skarbowiec, ul. Grójecka 41, 02-031 Warszawa
 - b. drogą mailową na adres: iod@skarbowiec.waw.pl
- 5) Administrator Danych Osobowych ma obowiązek zweryfikować osobę fizyczną, której dane dotyczą zgodnie z zakresem danych zawartym w specyfikacji niniejszej procedury.




- 6) Administrator odnosi się do żądania osoby fizycznej w terminie nie dłuższym niż 14 dni.
- 7) W przypadku, w którym realizacja prawa do sprzeciwu danych nie mogła zostać zrealizowana w terminie, Administrator wysyła osobie fizycznej, której dane dotyczą informację o przyczynach przedłużenia procesu.
- 8) Administrator zapewnia, że podczas obsługi realizacji praw związanych z prawem do sprzeciwu, nie narusza praw innych osób, w tym tajemnic handlowych, własności intelektualnej oraz praw autorskich chroniących oprogramowanie.

Specyfikacja:

Minimalny zakres danych niezbędnych do weryfikacji osoby, której dane dotyczą:

- imię, nazwisko, której zgłoszenie dotyczy oraz osoby zgłaszającej,
- opis zgłaszanego żądania wraz ze wskazaniem ewentualnych zastrzeżeń,
- podpis osoby zgłaszającej żądanie w przypadku zgłoszeń pisemnych,
- pełnomocnictwo, jeśli w imieniu zgłaszającego żądanie działa pełnomocnik,
- informacje o preferowanej formie odpowiedzi, jeżeli kanał odpowiedzi ma być inny niż zgłoszone żądanie.

W przypadku braku możliwości identyfikacji wnioskodawcy lub zaistnienia wątpliwości co do jego tożsamości, w celu zachowania bezpieczeństwa przetwarzanych danych osobowych, Administrator może zażądać dodatkowych danych potwierdzających tożsamość wnoszącego.

Wykaz zmian:

Edycja nr	Data edycji	Opis zmiany

MACIEJ CZYŃSKI

PREZES ZARZĄDU
SBM „SKARBOWIEC”



CZŁONEK ZARZĄDU
SBM „SKARBOWIEC”

SBM Skarbowiec	Nazwa dokumentu:			
	Procedura realizacji prawa do cofnięcia zgody			
	Edycja:	1	Obowiązuje od:	05.01.2021
	Uchwała nr	1/2021	Data uchwalenia:	05.01.2021
Zastępuje:	N/D			
<i>Własność SBM Skarbowiec. Do użytku wewnętrznego. Podlega nadzorowi.</i>				
Opracował		Zatwierdził		
Katarzyna Prokopowicz		Zarząd		

Cel procedury:

Procedura definiuje realizację prawa do cofnięcia zgody zgodnie z art. 7 RODO.

Wymagania:

- 1) W przypadku, gdy podstawą przetwarzania danych osobowych jest zgoda osoby fizycznej, osoba fizyczna ma prawo w dowolnym momencie wycofać zgodę na przetwarzanie danych osobowych.
- 2) Cofnięcie zgody nie wpływa na wcześniejszą zgodność z prawem przetwarzania danych, a wycofanie zgody musi być równie łatwe jak jej wyrażenie.
- 3) Żądania osób fizycznych w zakresie realizacji prawa do cofnięcia zgody może być kierowane:
 - a. drogą pisemną na adres: SBM Skarbowiec, ul. Grójecka 41, 02-031 Warszawa
 - b. drogą mailową na adres: iod@skarbowiec.waw.pl
- 4) Administrator Danych Osobowych ma obowiązek zweryfikować osobę fizyczną, której dane dotyczą zgodnie z zakresem danych zawartym w specyfikacji niniejszej procedury.
- 5) Administrator odnosi się do żądania osoby fizycznej w terminie nie dłuższym niż 14 dni.
- 6) W przypadku, w którym realizacja prawa do cofnięcia zgody nie mogła zostać zrealizowana w terminie, Administrator wysyła osobie fizycznej, której dane dotyczą informację o przyczynach przedłużenia procesu.
- 7) Administrator zapewnia, że podczas obsługi realizacji praw związanych z prawem do cofnięcia zgody, nie narusza praw innych osób, w tym tajemnic handlowych, własności intelektualnej oraz praw autorskich chroniących oprogramowanie.




Specyfikacja:


Minimalny zakres danych niezbędnych do weryfikacji osoby, której dane dotyczą:

- imię, nazwisko, której zgłoszenie dotyczy oraz osoby zgłaszającej,
- opis zgłaszanego żądania wraz ze wskazaniem ewentualnych zastrzeżeń,
- podpis osoby zgłaszającej żądanie w przypadku zgłoszeń pisemnych,
- pełnomocnictwo, jeśli w imieniu zgłaszającego żądanie działa pełnomocnik,
- informacje o preferowanej formie odpowiedzi, jeżeli kanał odpowiedzi ma być inny niż zgłoszone żądanie.

W przypadku braku możliwości identyfikacji wnioskodawcy lub zaistnienia wątpliwości co do jego tożsamości, w celu zachowania bezpieczeństwa przetwarzanych danych osobowych, Administrator może zażądać dodatkowych danych potwierdzających tożsamość wnoszącego.

Wykaz zmian:

Edycja nr	Data edycji	Opis zmiany

MACIEJ CZYŃSKI
PREZES ZARZĄDU
SBM „SKARBOWIEC”



ROBERT KRUPA
CZŁONEK ZARZĄDU
SBM „SKARBOWIEC”

SBM Skarbowiec	Nazwa dokumentu: Procedura postępowania w przypadku incydentów ochrony danych osobowych			
	Edycja:	1	Obowiązuje od:	05.01.2021
	Uchwała nr	1/2021	Data uchwalenia:	05.01.2021
	Zastępuje:	N/D		
<i>Własność SBM Skarbowiec. Do użytku wewnętrznego. Podlega nadzorowi.</i>				
Opracował		Zatwierdził		
Katarzyna Prokopowicz		Zarząd		

Cel procedury:

Procedura definiuje katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reakcji na naruszenia ochrony danych osobowych. Jej celem jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

Wymagania:

- 1) Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadomienia bezpośredniego przełożonego o stwierdzeniu podatności lub wystąpieniu incydu.
- 2) Przełożony zawiadamia Administratora Danych Osobowych.
- 3) W przypadku stwierdzenia wystąpienia incydu, Administrator Danych Osobowych jest zobowiązany do przeprowadzenia postępowania wyjaśniającego, które doprowadzi do:
 - ustalenia zakresu incydu,
 - ustalenia przyczyn incydu,
 - ustalenia skutków incydu.
- 4) Po przeprowadzeniu postępowania Administrator Danych Osobowych:
 - proponuje i wyciąga ewentualne działania dyscyplinarne,
 - proponuje działania na rzecz przywrócenia stanu organizacji przed wystąpieniem incydu,
 - rekomenduje działania prewencyjne zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich wystąpienia.
- 5) Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, z uwzględnieniem okoliczności naruszenia ochrony danych osobowych, jego skutków oraz podjętych działań zaradczych.

Am.

u

- 6) Osobom upoważnionym do przetwarzania danych osobowych zabrania się świadomego lub nieumyślnego wywoływania incydentów.
- 7) W stosunku do osób, które dopuściły się świadomego lub nieumyślnego wywoływania incydentów mogą zostać wyciągnięte konsekwencje prawne oraz organizacyjne.
- 8) W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki podejmuje działania zgodne z Procedurą zgłaszania naruszeń ochrony danych osobowych do Urzędu Ochrony Danych Osobowych.

Specyfikacja:

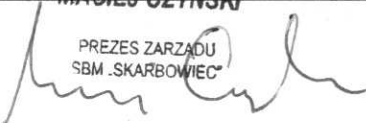

Do przykładowych podatności bezpieczeństwa danych osobowych należą:

- niewłaściwe zabezpieczenie pomieszczeń, urządzeń i dokumentów,
- niewłaściwe zabezpieczenie sprzętu IT oraz oprogramowania,
- nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu/drukarki, ochrony i polityki haseł, niezamykanie pomieszczeń, szaf, biurek),
- wykonywanie obowiązków służbowych przy wykorzystaniu komputera prywatnego i/lub telefonu prywatnego bez poddania ich uprzedniemu sprawdzeniu i zabezpieczeniu zgodnie z §10 i §14 Instrukcji Zarządzania Systemami Informatycznymi.

Do typowych incydentów bezpieczeństwa danych osobowych należą:

- zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
- zdarzenie losowe wewnętrzne (awarie serwera, komputerów, twardej dysków, oprogramowania, pomyłki, utrata/zagubienie danych),
- umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i in.).

Wykaz zmian:

Edycja nr	Data edycji	Opis zmiany
		<div style="display: flex; justify-content: space-between; align-items: center;"> <div style="text-align: center;">  MACIEJ GZYŃSKI PREZES ZARZĄDU SBM „SKARBOWIEC” </div> <div style="text-align: center;">  ROBERT KRUPA CZŁONEK ZARZĄDU SBM „SKARBOWIEC” </div> </div>

SBM Skarbowiec	Nazwa dokumentu: Procedura zgłaszania naruszeń ochrony danych osobowych do Urzędu Ochrony Danych Osobowych			
	Edycja:	1	Obowiązuje od:	05.01.2021
	Uchwała nr	1/2021	Data uchwalenia:	05.01.2021
	Zastępuje:	N/D		
<i>Własność SBM Skarbowiec. Do użytku wewnętrznego. Podlega nadzorowi.</i>				
Opracował		Zatwierdził		
Katarzyna Prokopowicz		Zarząd		

Cel procedury:

Procedura opisuje proces zgłaszania naruszenia ochrony danych osobowych do organu nadzorczego zgodnie z art. 33 RODO.

Wymagania:

- 1) W przypadku wystąpienia naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych Zarząd obowiązany do dokonania zgłoszenia incydentu do Urzędu Ochrony Danych Osobowych w terminie nie dłuższym niż 72h od dnia otrzymania informacji o incydencie.
- 2) Zgłoszenie naruszenia ochrony danych zawierać informacje określone w art. 33 ust. 3 RODO oraz specyfikacji do niniejszej procedury.
- 3) Administrator Danych Osobowych dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.

Specyfikacja:

Zgłoszenie naruszenia ochrony danych, zgodnie z art. 33 ust. 3 RODO, musi co najmniej:

- opisywać charakter 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,





- zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
- opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,
- opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Wykaz zmian:

Edycja nr	Data edycji	Opis zmiany

MACIEJ CZYŃSKI
 PREZES ZARZĄDU
 SBM „SKARBOWIEC”



ROBERT KRUPA
 CZŁONEK ZARZĄDU
 SBM „SKARBOWIEC”



SBM Skarbowiec	Nazwa dokumentu: Procedura usuwania i niszczenia danych osobowych			
	Edycja:	1	Obowiązuje od:	05.01.2021
	Uchwała nr	1/2021	Data uchwalenia:	05.01.2021
	Zastępuje:	N/D		
<i>Własność SBM Skarbowiec. Do użytku wewnętrznego. Podlega nadzorowi.</i>				
Opracował		Zatwierdził		
Katarzyna Prokopowicz		Zarząd		

Cel procedury:

Procedura określa sposoby usuwania i niszczenia danych osobowych w formie papierowej i elektronicznej.

Wymagania:

- 1) Dokumentacja papierowa niszczona jest w niszczarkach paskowych stanowiących wyposażenie firmy.
- 2) W uzasadnionych przypadkach dokumentacja papierowa może być niszczona za pośrednictwem firmy zewnętrznej wyspecjalizowanej w niszczeniu dokumentacji. Firma zobowiązana jest do wykazania się bezpieczną procedurą utylizacji oraz podpisania umowy powierzenia przetwarzania danych osobowych.
- 3) W odniesieniu do wszystkich nośników danych osobowych stosowane są mechanizmy bezpiecznego kasowania informacji:
 - a. przy pomocy specjalistycznego oprogramowania lub
 - b. w procesie demagnetyzacji lub
 - c. poprzez fizyczne niszczenie (pocięcie, spalanie) nośników.
- 4) Administrator Danych Osobowych dokonuje regularnych kontroli prawidłowości usunięcia informacji.
- 5) Za właściwe skasowanie informacji zawartej na nośniku przenośnym lub w pamięci masowej stacji roboczej odpowiada użytkownik.

Cu

Ł

- 6) Za kasowanie informacji z pamięci masowych serwerów oraz nośników kopii archiwalnych i zapasowych odpowiada Administrator Danych Osobowych lub osoba przez niego wyznaczona.
- 7) W uzasadnionych przypadkach dokumentacja elektroniczna może być niszczona za pośrednictwem firmy zewnętrznej wyspecjalizowanej w niszczeniu dokumentacji. Firma zobowiązana jest do wykazania się bezpieczną procedurą utylizacji oraz podpisania umowy powierzenia przetwarzania danych osobowych.
- 8) Za podpisanie umowy powierzenia przetwarzania danych osobowych z firmami zewnętrznymi odpowiedzialny jest Administrator Danych Osobowych.

Wykaz zmian:

Edycja nr	Data edycji	Opis zmiany

MACIEJ CZYŃSKI
PREZES ZARZĄDU
SBM „SKARBOWIEC”



ROBERT KRUPA
CZŁONEK ZARZĄDU
SBM „SKARBOWIEC”