POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH W SPÓŁDZIELNI MIESZKANIOWEJ KASZUBY W KARTUZACH

SPIS TREŚCI.

I. Wstęp.....3

II. Definicje.....3

III. Polityka bezpieczeństwa w zakresie ochrony danych osobowych.....4

A) Ogólne zasady polityki bezpieczeństwa.….....4

B) Wykaz budynków i pomieszczeń w których przetwarzane są dane osobowe.....8

C) Kategorie Danych Osobowych……..….....12

D) Systemy informatyczne służące do przetwarzania danych…….....….....16

E) Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych.....16

IV. Opis zdarzeń naruszających ochronę danych osobowych.....18

V. Postępowanie w przypadku naruszenia ochrony danych osobowych.....….....19

VI. Postanowienia końcowe.....21

VII. Załączniki.....….21

Zał. 1) Wzór oświadczenia o zapoznaniu się z „Polityką bezpieczeństwa”

Zał. 2) Wzór upoważnienia do przetwarzania danych.

Zał. 3) Wzór oświadczenia o zachowaniu w poufności uzyskanych danych osobowych oraz sposobów ich zabezpieczenia

Zał. 4) Wzór rejestru czynności przetwarzania danych osobowych

Zał. 5) Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych

Zał. 6) Wzór oświadczenia o wyrażeniu zgody na przetwarzanie danych osobowych w tym danych wrażliwych

.

I. WSTĘP

Mając na uwadze, iż w Spółdzielni Mieszkaniowej Kaszuby w Kartuzach, uwzględniając specyfikę jej działalności, przetwarza się dane osobowe, Zarząd Spółdzielni działając zgodnie z wymaganiami 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) oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych ustanawia niniejszym „Politykę bezpieczeństwa danych osobowych" (zwaną dalej „Polityką bezpieczeństwa"). Zarząd Spółdzielni realizuje tym samym nie tylko obowiązki wynikające z przepisów prawa lecz także nadrzędny cel jakim jest zapewnienie rzeczywistej ochrony wszelkich przetwarzanych przez Spółdzielnię danych osobowych.

Niniejszy dokument ustanawia szereg wytycznych i zasad postępowania dla osób uczestniczących w procesie przetwarzania danych osobowych, jak również procedur na wypadek ich naruszenia, wskazując na metody zabezpieczenia danych przetwarzanych czy to w formie papierowej, czy za pomocą systemów informatycznych.

II. DEFINICJE

„Polityka bezpieczeństwa danych osobowych Spółdzielni Mieszkaniowej Kaszuby w Kartuzach stanowi zbiór zasad, reguł i praktycznych rozwiązań regulujących sposób przetwarzania, zarządzania, ochrony i dystrybucji danych osobowych wewnątrz Spółdzielni. Ilekroć w treści „Polityki bezpieczeństwa" jest mowa o:

Danych osobowych – rozumie się przez to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą").

Osobie możliwej do zidentyfikowania – rozumie się przez to osobę, 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;

Administratorze - rozumie się przez to Spółdzielnię Mieszkaniową Kaszuby w Kartuzach reprezentowaną przez Zarząd;

Spółdzielni - rozumie się przez to Spółdzielnię Mieszkaniową Kaszuby w Kartuzach;

Inspektorze Ochrony Danych Osobowych – rozumie się przez to osobę wyznaczoną do nadzorowania przestrzegania zasad ochrony danych osobowych określonych w „Polityce bezpieczeństwa" oraz zasad wynikających z powszechnie obowiązujących przepisów prawa.

Zbiorze danych - rozumie się przez uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie

Przetwarzaniu - rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

Stronie trzeciej – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;

Systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

Instrukcji zarządzania systemem informatycznym – rozumie się przez to instrukcję określającą sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji w Spółdzielni Mieszkaniowej Kaszuby w Kartuzach;

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

Usuwaniu danych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

III. POLITYKA BEZPIECZEŃSTWA W ZAKRESIE OCHRONY DANYCH OSOBOWYCH.

A) Ogólne zasady polityki bezpieczeństwa.

1. „Polityka bezpieczeństwa" obowiązuje wszystkie osoby uczestniczące w przetwarzaniu danych osobowych w Spółdzielni. Osoby te powinny złożyć oświadczenie o zapoznaniu się z treścią Polityki

bezpieczeństwa i dokumentów pochodnych oraz zobowiązać się do ich przestrzegania, a także do zachowania w tajemnicy uzyskanych danych osobowych oraz sposobów ich zabezpieczenia. (Zał. 1 do „Polityki bezpieczeństwa").

2. Wykonywanie postanowień „Polityki bezpieczeństwa" ma zapewnić właściwą reakcję, ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa w danym rejestrze zbioru danych osobowych w Spółdzielni.

3. Administrator nadaje pisemne upoważnienia do przetwarzania danych (stronie trzeciej) pracownikom oraz współpracownikom, którzy w ramach swoich obowiązków uczestniczą w przetwarzaniu danych osobowych w Spółdzielni. (Zał. 2 do „Polityki bezpieczeństwa"). Udzielone upoważnienie może zostać w każdej chwili odwołane.

4. Osoby które nie uczestniczą w przetwarzaniu danych osobowych, lecz uzyskują do nich dostęp (np. członkowie Rady Nadzorczej Spółdzielni, kontrahenci itp.), powinni złożyć pisemne oświadczenie o zachowaniu w tajemnicy uzyskanych danych osobowych oraz sposobów ich zabezpieczenia. (Zał. 3 do „Polityki bezpieczeństwa").

5. Administrator, wyznacza Inspektora Ochrony Danych Osobowych którego upoważnia pisemnie do przetwarzania danych osobowych, w związku z wykonywanymi obowiązkami.

6. Inspektor Ochrony Danych Osobowych zobowiązany jest do:

1) zapewniania przestrzegania przepisów o ochronie danych osobowych w Spółdzielni, w szczególności poprzez:

a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych,

b) nadzorowanie opracowywania i aktualizowania dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności, zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem oraz przestrzegania zasad w niej określonych,

c) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;

2) informowanie Administratora oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy przepisów o ochronie danych i doradzanie im w tej sprawie;

3) prowadzenia rejestru czynności przetwarzania danych osobowych; (Zał. 4 do „Polityki bezpieczeństwa")

4) opracowania i aktualizowania ewidencji osób upoważnionych do przetwarzania danych

osobowych; (Zał. 5 do „Polityki bezpieczeństwa")

5) przygotowywania i opiniowania projektów dokumentów wydawanych przez Administratora danych (w tym opracowania i aktualizowania dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną oraz odpowiedzi na pisma, uchwały, upoważnienia itp., których tematyka dotyczy bezpośrednio przetwarzania i ochrony danych osobowych);

7. „Polityka bezpieczeństwa" określa tryb postępowania w przypadku, gdy:
   a) stan urządzenia, zawartość rejestru czynności przetwarzania danych osobowych., ujawnione metody pracy mogą wskazywać na naruszenie zabezpieczeń tych danych,
   b) stwierdzono naruszenie bezpieczeństwa przetwarzanych danych.

8. W przypadku wykrycia naruszeń zasad ochrony danych osobowych lub nieuprawnionego dostępu do zbiorów danych osobowych przetwarzanych przez Spółdzielnię, Inspektor podejmuje konieczne działania, zgodne z wytycznymi „Polityki bezpieczeństwa" i niezwłocznie informuje Administratora o naruszeniu.

9. W przypadku zbierania nowych danych osobowych, pracownik Spółdzielni działający w jej imieniu, zobowiązany jest do sprawdzenia, czy na dokumencie na którym przekazywane są dane, zawarta została klauzula informacyjna dotycząca zgody na ich przetwarzanie.

10. W procesie rekrutacji pracowników dopuszczalne jest zbieranie danych osobowych jedynie w zakresie wynikającym z przepisu art. 22^1 kodeksu pracy. W wypadku gdy zakres danych przekracza ustawowy, a osoba nie wyraziła zgody na ich przetwarzanie, dane te powinny zostać usunięte.

11. W przypadkach zawierania przez Spółdzielnię umów, których wykonanie wiąże się z przekazywaniem do przetwarzania danych osobowych innemu podmiotowi, Spółdzielnia zawiera z tym podmiotem pisemną umowę powierzającą przetwarzanie danych osobowych ze zbiorów Spółdzielni.

12. Administrator wprowadza przygotowaną przez Inspektora „Instrukcję zarządzania systemem informatycznym", określającą sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji w Spółdzielni.

13. Administrator wprowadza przygotowaną przez Administratora bezpieczeństwa informacji „Instrukcję w sprawie zasad postępowania przy przetwarzaniu danych osobowych" określającą w sposób szczegółowy obowiązki osób upoważnionych do przetwarzania danych osobowych w Spółdzielni.

14. Osobom, których dane są przetwarzane przez Spółdzielnię przysługuje prawo do kontroli przetwarzania danych, zgodnie z regułami zawartymi ROZPORZĄDZENIU PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

15. Dane osobowe udostępnia się na pisemny, umotywowany wniosek. Wniosek powinien zawierać informacje umożliwiające wyszukanie danych osobowych oraz wskazywać ich zakres i przeznaczenie. Udostępnione dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

16. Jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą, administrator podaje osobie, której dane dotyczą, następujące informacje:

a) swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;

b) gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych;

c) cele przetwarzania, do których mają posłużyć dane osobowe, oraz podstawę prawną przetwarzania;

d) kategorie odnośnych danych osobowych;

e) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;

17. Poza informacjami, o których mowa w ust. 16, administrator podaje osobie, której dane dotyczą, następujące informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania wobec osoby, której dane dotyczą:

a) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;

b) jeżeli przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności

gdy osoba, której dane dotyczą, jest dzieckiem – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;

c) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;

d) informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;

e) informacje o prawie wniesienia skargi do organu nadzorczego;

f) źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych;

18. Informacje, o których mowa w ust. 16 i 17, administrator podaje:

a) w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca – mając na uwadze konkretne okoliczności przetwarzania danych osobowych;

b) jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą; lub

c) jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.

19. Jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym te dane zostały pozyskane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji.

20. Czas przechowywania przez administratora danych osobowych zależny jest od ich rodzaju i określony w rejestrze czynności przetwarzania danych osobowych.

B) Wykaz budynków i pomieszczeń w których przetwarzane są dane osobowe.

SIEDZIBA SPÓŁDZIELNI znajduje się w wolnostojącym budynku parterowym położonym w Kartuzach przy ul. Sędzickiego 30, nieruchomość stanowi własność Spółdzielni. Do części biurowej siedziby prowadzą dwa wejścia, pierwsze zabezpieczone jest metalowymi drzwiami zewnętrznymi z szybą oraz dwoma zamkami patentowymi oraz plastikowe drzwi wewnętrzne z szyba i jednym zamkiem

patentowym natomiast drugie wejście zabezpieczone jest metalowymi drzwiami zewnętrznymi z szybą oraz dwoma zamkami patentowymi. Do części technicznej siedziby prowadzą trzy wejścia zabezpieczone w następujący sposób: 1. pełne drzwi metalowe z dwoma zamkami patentowymi 2. pełne drzwi metalowe z zamkiem patentowym i ryglami zamykanymi od wewnątrz 3. pełne drzwi metalowe z ryglami zamykanymi od wewnątrz. Okna w pomieszczeniu 'KASA' są zabezpieczone są zewnętrznymi kratami bez możliwości otwierania. W siedzibie Spółdzielni funkcjonuje alarm antywłamaniowy. Dostęp do kluczy do Siedziby Spółdzielnia mają Administrator, Specjalista ds. zasobów lokalowych, Specjalista ds. inwestycji i remontów oraz sprzątaczka biurowa. Klucze do poszczególnych pomieszczeń przechowywane są w pomieszczeniu **Sekretariatu** w przeznaczonej do tego celu gablotce, dostęp do nich mają pracownicy Spółdzielni mający dostęp do poszczególnych pomieszczeń.

Siedziba Spółdzielni składa się z następujących pomieszczeń, w których przetwarzane są dane osobowe:

1. **Pokój Specjalistów ds. zasobów lokalowych (2D)** - znajduje się za sekretariatem po lewej stronie korytarza, prowadzą do niego drzwi zabezpieczone zamkiem, w pomieszczeniu znajdują się szafy drewniane do przechowywania dokumentacji częściowo zabezpieczone zamkiem oraz dwie stacje robocze (komputery). Dostęp do pomieszczenia mają osoby zatrudnione na stanowisku Specjalistów ds. zasobów lokalowych, pozostali pracownicy Spółdzielni oraz osoby trzecie - w obecności wskazanych pracowników.
2. **Pokój Radcy Prawnego (2C)** – pomieszczenie znajduje się za sekretariatem po prawej stronie korytarza, prowadzą do niego drzwi zabezpieczone zamkiem, w pomieszczeniu znajdują się szafy drewniane do przechowywania dokumentacji częściowo zabezpieczone zamkiem oraz jedna stacja robocza (komputer). Dostęp do pomieszczenia mają pozostali pracownicy Spółdzielni oraz osoby trzecie - w obecności wskazanych pracowników oraz Radca Prawny.
3. **Sekretariat (Specjalista) (2)** - pomieszczenie znajduje na końcu korytarza po lewej stronie za wejściem do siedziby Spółdzielni, prowadzą do niego drzwi zabezpieczone zamkiem, w pomieszczeniu znajdują się szafki drewniane do przechowywania dokumentacji częściowo zabezpieczone zamkiem, a także jedna stacja robocza (komputer). Dostęp do pomieszczenia mają Prezes Zarządu, oraz osoba zatrudniona na stanowisku Specjalisty ds. administracyjno-pracowniczych, pozostali pracownicy Spółdzielni oraz osoby trzecie - w obecności wskazanych pracowników.
4. **Gabinet Prezesa Zarządu (2B)** - pomieszczenie znajduje się po lewej stronie od wejścia do sekretariatu, prowadzą do niego drzwi zabezpieczone zamkiem, w pomieszczeniu znajdują się szafy drewniane do przechowywania dokumentacji częściowo zabezpieczone zamkiem oraz jedna stacja

robocza (komputer). Dostęp do pomieszczenia ma Prezes Zarządu Spółdzielni, pozostali pracownicy Spółdzielni oraz osoby trzecie - w obecności Prezesa.

5. **Gabinet Głównej Księgowej (2A) -** pomieszczenie znajduje się po lewej stronie wejścia do Sekretariatu obok wejścia do Gabinetu Prezesa Zarządu prowadzą do niego drzwi zabezpieczone zamkiem, z pomieszczenia prowadzi przejście do pomieszczenia pokoju Księgowości (Specjaliści) z drzwiami zabezpieczonymi zamkiem, w pomieszczeniu znajdują się szafki i szafy drewniane do przechowywania dokumentacji częściowo zabezpieczone zamkiem, a także dwie stacje robocze (komputery). Dostęp do pomieszczenia mają Główna Księgowa oraz osoba zatrudniona na stanowisku Specjalista ds. finansowych, pozostali pracownicy Spółdzielni i osoby trzecie - w obecności Głównej Księgowej.

6. **Księgowość (Specjaliści) (1)** - pomieszczenie znajduje się po lewej stronie korytarza za wejściem do siedziby Spółdzielni i jest połączone z Gabinetem Głównej Księgowej, prowadzą do niego dwoje drzwi zabezpieczone zamkiem, w pomieszczeniu znajdują się szafki i szafy drewniane do przechowywania dokumentacji częściowo zabezpieczone zamkiem, a także dwie stacje robocze (komputery). Dostęp do pomieszczenia mają Główna Księgowa oraz osoby zatrudnione na stanowiskach Specjalistów ds. finansowych, pozostali pracownicy Spółdzielni i osoby trzecie – w obecności wskazanych pracowników.

7. **Księgowość (Specjalista) (7)** - pomieszczenie znajduje się po prawej stronie korytarza za wejściem do siedziby Spółdzielni naprzeciwko pomieszczenia Kasa-Kasjer, prowadzą do niego drzwi zabezpieczone zamkiem, z pomieszczenia prowadzi przejście do pomieszczenia Administracji (Specjaliści) z drzwiami zabezpieczonymi zamkiem, w pomieszczeniu znajdują się szafy drewniane do przechowywania dokumentacji częściowo zabezpieczone zamkiem oraz jedna stacja robocza (komputer). Dostęp do pomieszczenia ma osoba zatrudniona na stanowisku Specjalisty ds. rozliczeń mediów, pozostali pracownicy Spółdzielni oraz osoby trzecie - w obecności wskazanych pracowników.

8. **Kadry i Płace (2C) -** znajduje się za sekretariatem po prawej stronie korytarza, prowadzą do niego drzwi zabezpieczone zamkiem, w pomieszczeniu znajdują się szafy drewniane do przechowywania dokumentacji częściowo zabezpieczone zamkiem oraz jedna stacja robocza (komputer). Dostęp do pomieszczenia ma osoba zatrudniona na stanowisku Specjalisty ds. kadr i płac, pozostali pracownicy Spółdzielni oraz osoby trzecie - w obecności wskazanych pracowników.

9. **Serwer -** pomieszczenie znajduje się za pomieszczeniem pokoju Księgowości , prowadzą do niego drzwi zabezpieczone zamkiem, w pomieszczeniu znajduje się serwer HP Proliant ML310 (RAID-1,

Windows Server 2003R2) oraz dysk sieciowy (NAS). Klucz do pomieszczenia znajduje się w Sekretariacie i jest udostępniany w razie konieczność informatykowi.

10. **Kasa (3) -** pomieszczenie znajduje się po lewej stronie korytarza za wejściem do siedziby Spółdzielni naprzeciwko pomieszczenia pokoju Księgowości (Specjalista), prowadzą do niego metalowe drzwi zabezpieczone dwoma zamkami w pomieszczeniu znajdują się szafy drewniane do przechowywania dokumentacji częściowo zabezpieczone zamkiem, sejf oraz jedna stacja robocza (komputer). Dostęp do pomieszczenia ma osoba zatrudniona na stanowisku Kasjera, pozostali pracownicy Spółdzielni oraz osoby trzecie - w obecności wskazanych pracowników.
11. **Techniczny (Specjaliści) (4)** - pomieszczenie znajduje się po prawej stronie korytarza za pomieszczeniem Kasa – Kasjer, prowadzą do niego drzwi zabezpieczone zamkiem, w pomieszczeniu znajdują się szafki i szafy drewniane do przechowywania dokumentacji częściowo zabezpieczone zamkiem a także dwie stacje robocze (komputery). Dostęp do pomieszczenia mają osoby zatrudnione na stanowisku Specjalisty ds. technicznych, Specjalisty ds. inwestycji i remontów, pozostali pracownicy Spółdzielni i osoby trzecie - w obecności wskazanych pracowników.
12. **Administracja (Specjaliści) (6) -** pomieszczenie znajduje się po prawej stronie korytarza za pomieszczeniem pokoju Księgowości naprzeciwko pomieszczenia pokoju Technicznego, prowadzą do niego drzwi zabezpieczone zamkiem, w pomieszczeniu znajdują się szafki i szafy drewniane do przechowywania dokumentacji częściowo zabezpieczone zamkiem a także dwie stacje robocze (komputery). Dostęp do pomieszczenia mają osoby zatrudnione na stanowisku Administratora, Specjalisty ds. zasobów lokalowych oraz Specjalisty ds. rozliczania c.o i c.w.u. (umowa zlecenie), pozostali pracownicy Spółdzielni i osoby trzecie - w obecności wskazanych pracowników.
13. **Archiwum –** dwa pomieszczenia znajdujące się w części technicznej siedziby Spółdzielni na końcu korytarza pomiędzy pomieszczeniem socjalnym a pomieszczeniem warsztatów, do pomieszczeń prowadzą drzwi zabezpieczone zamkiem, w pomieszczeniach znajduje się gaśnica, dostęp do archiwum maja pracownicy Spółdzielni.

C) Kategorie Danych Osobowych

W Spółdzielni prowadzi się rejestr czynności przetwarzania danych osobowych w oparciu o określone poniżej kategorie danych osobowych.

1. **Członkowie Spółdzielni -** zbiór zawierający dane członków Spółdzielni, w tym członków

posiadających tytuły prawne do lokali, obejmujący dane osobowe przetwarzane w następującym zakresie:

a) dane identyfikacyjne członków (imiona i nazwiska, adres zamieszkania i/lub adres do korespondencji, numer ewidencyjny PESEL, dodatkowe dane kontaktowe (telefon/mail), data powstania członkostwa);
b) informacje o lokalu do którego członkowi przysługuje tytuł prawny (data nabycia, adres, powierzchnia, wysokość opłat);
c) dane osób zamieszkujących w lokalu wraz z członkiem (imiona i nazwiska, adres zamieszkania, dodatkowe dane kontaktowe (telefon/mail);

2. KANDYDACI NA CZŁONKÓW SPÓŁDZIELNI – zbiór zawierający dane osób które wystąpiły z wnioskiem o przyjęcie w poczet członków Spółdzielni, obejmujący dane osobowe przetwarzane w następującym zakresie:

a) dane identyfikacyjne kandydata (imiona i nazwiska, adres zamieszkania lub adres do korespondencji, numer ewidencyjny PESEL, dodatkowe dane kontaktowe (telefon/mail)
b) informacje o lokalu do którego kandydatowi przysługuje tytuł prawny (data nabycia, adres, powierzchnia)

3. WŁAŚCICIELE LOKALI NIE BĘDĄCY CZŁONKAMI SPÓŁDZIELNI - zbiór zawierający dane osób którym przysługuje tytuł prawny do lokalu, a które nie są członkami Spółdzielni, obejmujący dane osobowe przetwarzane w następującym zakresie:

a) dane identyfikacyjne właściciela (imiona i nazwiska, adres zamieszkania lub adres do korespondencji, numer ewidencyjny PESEL, dodatkowe dane kontaktowe (telefon/mail), data powstania członkostwa);
b) informacje o lokalu do którego właścicielowi przysługuje tytuł prawny (data nabycia, adres, powierzchnia, wysokość opłat);
c) dane osób zamieszkujących w lokalu wraz z właścicielem (imiona i nazwiska, adres zamieszkania, dodatkowe dane kontaktowe (telefon/mail);

4. OSOBY ZAJMUJĄCE LOKALE BEZ TYTUŁU PRAWNEGO - zbiór zawierający dane osób zajmujących lokale stanowiące własność Spółdzielni, którym nie przysługuje tytuł prawny do lokalu, obejmujący dane osobowe przetwarzane w następującym zakresie:

a) dane identyfikacyjne lokatora (imiona i nazwiska, adres zamieszkania lub adres do korespondencji, numer ewidencyjny PESEL, dodatkowe dane kontaktowe (telefon/mail), data ustania członkostwa);

b) informacje o lokalu zajmowanym przez lokatora (data nabycia, adres, powierzchnia, wysokość opłat);
c) dane osób zamieszkujących w lokalu wraz z lokatorem (imiona i nazwiska, adres zamieszkania, dodatkowe dane kontaktowe (telefon/mail);

5. NAJEMCY LOKALI STANOWIĄCYCH WŁASNOŚĆ SPÓŁDZIELNI - zbiór zawierający dane osób z którymi Spółdzielnia zawarły umowy najmu lub dzierżawy, obejmujący dane osobowe przetwarzane w następującym zakresie:

a) dane identyfikacyjne najemcy/dzierżawcy (imiona i nazwiska, adres zamieszkania lub adres do korespondencji, numer ewidencyjny PESEL, numer ewidencyjny NIP, numer ewidencyjny REGON, dodatkowe dane kontaktowe (telefon/mail);
b) informacje o wynajmowanym lokalu lub dzierżawionym gruncie (data nabycia, adres, powierzchnia, wysokość opłat);
c) dane osób zamieszkujących w lokalu wraz z najemcą (imiona i nazwiska, adres zamieszkania, dodatkowe dane kontaktowe (telefon/mail) – dotyczy najemców lokali mieszkalnych

6. DZIERŻAWCY GRUNTÓW STANOWIĄCYCH WŁASNOŚĆ SPÓŁDZIELNI - zbiór zawierający dane osób z którymi Spółdzielnia zawarły umowy najmu lub dzierżawy, obejmujący dane osobowe przetwarzane w następującym zakresie:

a) dane identyfikacyjne najemcy (imiona i nazwiska, adres zamieszkania lub adres do korespondencji, numer ewidencyjny PESEL, numer ewidencyjny NIP, numer ewidencyjny REGON, dodatkowe dane kontaktowe (telefon/mail);
b) informacje o wynajmowanym lokalu (data nabycia, adres, powierzchnia, wysokość opłat);
c) dane osób zamieszkujących w lokalu wraz z najemcą (imiona i nazwiska, adres zamieszkania, dodatkowe dane kontaktowe (telefon/mail) – dotyczy najemców lokali mieszkalnych

7. PRACOWNICY SPÓŁDZIELNI - zbiór zawierający dane osób zatrudnionych w Spółdzielni, obejmujący dane osobowe przetwarzane w następującym zakresie:

a) dane identyfikacyjne pracowników (imiona i nazwiska, imiona rodziców, data urodzenia, adres zamieszkania lub adres do korespondencji, nr rachunku bankowego, numer ewidencyjny PESEL, numer ewidencyjny NIP, dodatkowe dane kontaktowe (telefon/mail), inne dane osobowe na podstawie przepisu art. 22^1 § 2 pkt 1 kodeksu pracy.)
b) dane dotyczące właściwości pracownika (posiadane kwalifikacje zawodowe, informacje o stanie zdrowia, historia zatrudnienia, skończone dodatkowe kursy i szkolenia)

c) informacje dotyczące wynagrodzenia pracowników (wysokość wynagrodzenia w tym otrzymanych premii, wysokość odprowadzanego podatku dochodowego, wysokość składek na ubezpieczenie społeczne, otrzymane kary finansowe)

8. KANDYDACI DO PRACY W SPÓŁDZIELNI - zbiór zawierający dane osób, które są kandydatami do pracy w Spółdzielni, obejmujący dane osobowe przetwarzane w następującym zakresie:

a) dane identyfikacyjne kandydatów (imiona i nazwiska, imiona rodziców, data urodzenia, adres zamieszkania lub adres do korespondencji, dodatkowe dane kontaktowe (telefon/mail))
b) dane dotyczące właściwości kandydata (posiadane kwalifikacje zawodowe, historia zatrudnienia, skończone dodatkowe kursy i szkolenia)

9. DŁUŻNICY - zbiór zawierający dane osób zobowiązanych do uiszczania opłat za lokale mieszkalne, które posiadają zadłużenie względem Spółdzielni, obejmujący dane osobowe przetwarzane w następującym zakresie:

a) dane identyfikacyjne dłużnika (imiona i nazwiska, data urodzenia, imiona rodziców, adres zamieszkania lub adres do korespondencji, numer ewidencyjny PESEL, dodatkowe dane kontaktowe (telefon/mail);
b) informacje o lokalu w związku z którym powstała zaległość dłużnika (adres, powierzchnia, wysokość opłat);
c) informacja o zadłużeniu dłużnika (wysokość zadłużenia podstawowego, wysokość odsetek, wezwania do zapłaty)

10. DŁUŻNICY – SPRAWY SĄDOWE I EGZEKUCYJNE - zbiór zawierający dane osób, których sprawy zostały przekazane na drogę postępowania sądowego i egzekucyjnego, obejmujący dane osobowe przetwarzane w następującym zakresie:

a) dane identyfikacyjne dłużnika (imiona i nazwiska, data urodzenia, imiona rodziców, adres zamieszkania lub adres do korespondencji, numer ewidencyjny PESEL, numer ewidencyjny NIP, numer ewidencyjny REGON, dodatkowe dane kontaktowe (telefon/mail);
b) informacje o lokalu w związku z którym powstała zaległość dłużnika (adres, wysokość opłat);
c) informacja o zadłużeniu dłużnika (wysokość zadłużenia podstawowego, wysokość odsetek, wezwania do zapłaty)
d) informacje o postępowaniu sądowym wszczętym przeciwko dłużnikowi (data wniesienia pozwu, data wydania nakazu zapłaty, data wniesienia sprzeciwu, data uprawomocnienia się

wyroku, wysokość należności ubocznych zasądzonych wyrokiem)

e) informacje o postępowaniu egzekucyjnym wszczętym przeciwko dłużnikowi (data wszczęcia egzekucji, zajęcia składników majątku dłużnika, dane dotyczące dłużnika i jego majątku ustalone przez komornika – miejsce pracy, nr rachunku bankowego, posiadane ruchomości i nieruchomości, inne posiadane wierzytelności)

11. **WSPÓŁPRACOWNICY SPÓŁDZIELNI -** zbiór zawierający dane współpracowników Spółdzielni nie prowadzących działalności gospodarczej, działających na podstawie umów cywilnoprawnych, obejmujący dane osobowe przetwarzane w następującym zakresie:
    a) dane identyfikacyjne współpracownika (imiona i nazwiska, data urodzenia, adres zamieszkania lub adres do korespondencji, nr rachunku bankowego, numer ewidencyjny PESEL, numer ewidencyjny NIP, dodatkowe dane kontaktowe (telefon/mail))
    b) dane dotyczące właściwości współpracownika (posiadane kwalifikacje, skończone dodatkowe kursy i szkolenia)
    c) informacje dotyczące wynagrodzenia pracowników (wysokość wynagrodzenia, wysokość odprowadzanego podatku dochodowego, wysokość składek na ubezpieczenie społeczne)

12. **KONTRAHENCI SPÓŁDZIELNI -** zbiór zawierający dane kontrahentów Spółdzielni, wykonujących zlecone zadania w ramach prowadzonej przez Spółdzielnię działalności gospodarczej, obejmujący dane osobowe przetwarzane w następującym zakresie:
    a) dane identyfikacyjne kontrahentów (imiona i nazwiska, firma działalności gospodarczej, adres siedziby lub adres do korespondencji, nr rachunku bankowego, numer ewidencyjny PESEL, numer ewidencyjny NIP, numer ewidencyjny REGON, dodatkowe dane kontaktowe (telefon/mail))
    b) dane dotyczące właściwości kontrahenta (przedmiot prowadzonej działalności gospodarczej, posiadane uprawnienia zawodowe, posiadane zezwolenia, ilość zatrudnianych pracowników, referencje)
    c) informacje dotyczące wynagrodzenia kontrahentów (wysokość wynagrodzenia, wysokość podatku VAT)

13. **OSOBY FIZYCZNE -** zbiór zawierający dane zbierane w ramach prowadzonego monitoringu wizyjnego budynku siedziby Spółdzielni oraz obszaru wokół, obejmujący dane osobowe przetwarzane w następującym zakresie danych identyfikacji wizyjnej - nagrania z monitoringu.

D) Systemy informatyczne służące do przetwarzania danych

1. DOM 5 (moduły: FK; zasoby; banki; kasa; kadry; płace; kredyty; obsługa techniczna nieruchomości; pozostała sprzedaż; windykacje; zakup; rejestr VAT; dział członkowski; wkłady i udziały; wspólnoty; czynsze lokali mieszkalnych; czynsze lokali użytkowych, media; koszty) - system zainstalowany jest na serwerze znajdującym się w pomieszczeniu serwer w siedzibie Spółdzielni. System zbudowany jest w architekturze trójwarstwowej i wykorzystuje bazę danych SQL. Do baz danych nie ma bezpośredniego dostępu z poziomu konta użytkownika. Do serwera głównego mogą logować się tylko zdefiniowani przez informatyka użytkownicy. Do zalogowania wymagany jest login oraz hasło. Konta przydzielone użytkownikom mają ograniczone uprawnienia.

2. Płatnik ZUS - system zainstalowany jest na stacji roboczej (komputerze) w pomieszczeniu Główna księgowa (nr 1) w siedzibie Spółdzielni. System wykorzystuje bazę danych Access, także znajdującą się na tej stacji roboczej. Dostęp do programu, jak i komputera, chroniony jest loginem i hasłem.

3. Edytory tekstu – poszczególne programy (systemy) zainstalowane są na danych stacjach roboczych, w siedzibie Spółdzielni. Pliki przechowywane są na dyskach lokalnych poszczególnych stacji roboczych (komputerów) zabezpieczonych loginem i hasłem.

4. Arkusze kalkulacyjne – poszczególne programy (systemy) zainstalowane są na danych stacjach roboczych, w siedzibie Spółdzielni. Pliki przechowywane są na dyskach lokalnych poszczególnych stacji roboczych (komputerów) zabezpieczonych loginem i hasłem.

5. Poczta elektroniczna – poszczególne programy (systemy) zainstalowane są na danych stacjach roboczych, w siedzibie Spółdzielni. Pliki przechowywane są na dyskach lokalnych poszczególnych stacji roboczych (komputerów) zabezpieczonych loginem i hasłem.

E) Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych.

1. Środki organizacyjne

Administrator , w celu zapewnieniu poufności, integralności i rozliczalności przy przetwarzaniu danych osobowych, stosuje następujące środki organizacyjne:

a) opracowanie i wdrożenie „Polityki bezpieczeństwa danych osobowych w Spółdzielni Mieszkaniowej Kaszuby w Kartuzach”;
b) opracowanie i wdrożenie „Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Spółdzielni Mieszkaniowej Kaszuby w

Kartuzach";

c) opracowanie i wdrożenie „Instrukcji w sprawie zasad postępowania przy przetwarzaniu danych osobowych";
d) nadanie przez Administratora upoważnień do przetwarzania danych osobowych wszystkim osobom uczestniczącym tym procesie;
e) prowadzenie przez Inspektora Ochrony Danych Osobowych dokumentacji w zakresie ochrony danych osobowych, wskazanej w treści Polityki bezpieczeństwa danych osobowych;
f) sprawowanie przez Inspektora Ochrony Danych Osobowych kontroli i nadzoru nad procesem przetwarzania danych osobowych;
g) zapoznanie osób upoważnionych do przetwarzania danych osobowych z treścią Polityki bezpieczeństwa oraz z przepisami o ochronie danych osobowych;

2. Środki techniczne:

Administrator danych w celu zapewnienia poufności, integralności, rozliczalności i ochrony przy przetwarzaniu danych osobowych stosuje następujące środki techniczne:

a) dokumentacja zawierająca dane osobowe przetwarzana w formie tradycyjnej (papierowej) przechowywana jest w pomieszczeniach zabezpieczonych kluczem, w przeznaczonych do tego szafach w siedzibie Spółdzielni, do których dostęp maja jedynie osoby upoważnione do przetwarzania danych osobowych;
b) w siedzibie Spółdzielni działa systemem monitoringu antywłamaniowego;
c) w celu ochrony dokumentacji w Spółdzielni obowiązuje instrukcja przeciwpożarowa;
d) stacje robocze, na których przetwarza się dane osobowe w systemie informatycznym pracują na systemach operacyjnych Windows xp, Windows 7 Home Premium, Windows 7 Professional oraz Windows 10. Chronione są loginem i hasłem, a dodatkowo zabezpieczone systemowym firewallem oraz oprogramowaniem antywirusowym Eset NOD 32 Antivirus;
e) do serwerów stanowiącego podstawę sieci LAN Spółdzielni, logować mogą się tylko zdefiniowani przez informatyka użytkownicy. Do zalogowania wymagany jest login oraz hasło. Konta przydzielone użytkownikom mają ograniczone uprawnienia. Sieć chroniona jest przez firewalle systemu MS Windows Server 2003R2;
f) systemy informatyczne, za pomocą których przetwarzane są dane osobowe mają własne zabezpieczenia, to jest dostęp do nich możliwy jest tylko dla osób uprawnionych po podaniu loginu i hasła;
g) przelewy bankowe i międzybankowe dokonywane z rachunków bankowych Spółdzielni wymagają podania loginu i hasła, a dostęp do rachunków posiadają jedynie osoby upoważnione;

h) dane osobowe przetwarzane za pomocą systemów informatycznych archiwizowane są zgodnie z wytycznymi zawartymi w Instrukcji zarządzania systemem informatycznym;

i) osoby uczestniczące w procesie przetwarzana danych osobowych w systemie informatycznym obowiązane są do wylogowania się przed opuszczeniem stanowiska pracy,

j) monitory stacji roboczych (komputerów), na których przetwarzane są dane osobowe ustawione są w taki sposób, aby nie dopuścić do wglądu w przetwarzane dane osobom postronnym;

IV. OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH OSOBOWYCH.

1. Podział zagrożeń mogących naruszać ochronę danych osobowych:

1) Zagrożenia losowe:

a) zewnętrzne (np. pożar, zalanie, awaria zasilania), mogące prowadzić do utraty danych w systemach informatycznych, zniszczenia infrastruktury technicznej – zostaje zakłócone funkcjonowanie systemów, lecz nie dochodzi do naruszenia poufności danych.

b) wewnętrzne (np. pomyłki operatorów, administratora, awarie sprzętu, błędy oprogramowania), mogące prowadzić do zniszczenia danych, zakłócenia ciągłość pracy systemów, a także do naruszenia poufności danych.

2) Zagrożenia zamierzone i celowe – wysokie zagrożenie naruszenia poufności danych. Zagrożenia te możemy podzielić na:

a) nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu),

b) nieuprawniony dostęp do systemu z jego wnętrza,

c) nieuprawniony przekaz danych,

d) pogorszenie jakości sprzętu i oprogramowania,

e) bezpośrednie zagrożenie materialnych składników systemu.

2. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe, to głównie:

1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np. wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.;

2) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych;

3) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie

w kierunku naruszenia ochrony danych;

4) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu;

5) pogorszenie jakości danych w systemie lub inne odstępstwo od stanu oczekiwanego, wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie;

6)naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie;

7) stwierdzona próba modyfikacji lub modyfikacja danych lub zmiana w strukturze danych, bez odpowiedniego upoważnienia (autoryzacji);

8) niedopuszczalna manipulacja danymi osobowymi w systemie;

9) ujawnienie osobom nieupoważnionym danych osobowych lub objętych tajemnicą procedur ochrony przetwarzania albo innych strzeżonych elementów systemu zabezpieczeń;

10) nieprzypadkowe odstępstwa od zasad bezpieczeństwa pracy w systemie lub sieci komputerowej, wskazujące na przełamanie lub zaniechanie ochrony danych osobowych, np. praca przy komputerze lub w sieci osoby nieupoważnionej;

11) istnienie nieautoryzowanych kont dostępu do danych;

12) podmiana lub zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia, jak również skasowanie lub skopiowanie w sposób niedozwolony danych osobowych;

13) rażące naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce lub na ksero, niezamknięcie pomieszczenia z komputerem, niewykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych itp.).

3. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) w formach tradycyjnych, (np. akta, wydruki, zdjęcia itp.).

V. POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH.

1. W przypadku stwierdzenia :

1) naruszenia zabezpieczeń systemu informatycznego,
2) naruszenia technicznego stanu urządzeń,
3) naruszenia zawartości zbioru danych osobowych,
4) ujawnienia metody pracy lub sposobu działania programu,
5) jakości transmisji danych w sieci telekomunikacyjnej, mogącej wskazywać na naruszenie

zabezpieczeń tych danych,

6) innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, itp.)

Każda osoba zatrudniona przy przetwarzaniu danych osobowych jest zobowiązana niezwłocznie powiadomić o tym fakcie Inspektora Ochrony Danych Osobowych.

2. W razie niemożliwości zawiadomienia Inspektora Ochrony Danych Osobowych należy powiadomić Zarząd Spółdzielni.

3. Do czasu przybycia na miejsce naruszenia danych osobowych Inspektora Ochrony Danych Osobowych, powinno się:

1) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu ustalenie przyczyn lub sprawców naruszenia danych osobowych;
2) udokumentować wstępnie zaistniałe naruszenie;
3) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora bezpieczeństwa informacji lub osoby przez niego upoważnionej.

4. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, Inspektor Ochrony Danych Osobowych:

1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania, mając na uwadze ewentualne zagrożenia dla prawidłowości pracy organizacji;
2) może żądać dokładnej relacji z zaistniałego naruszenia lub ujawnienia ochrony danych osobowych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem;
3) rozważa celowość i potrzebę powiadomienia o zaistniałym naruszeniu lub ujawnieniu ochrony danych osobowych Administratora danych;
4) nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza organizacji.

5. Po wyczerpaniu niezbędnych środków doraźnych, związanych z zaistniałym naruszeniem ochrony danych osobowych, Inspektora Ochrony Danych Osobowych zasięga niezbędnych opinii i proponuje postępowanie naprawcze, w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.

6. Inspektor Ochrony Danych Osobowych dokumentuje zaistniały przypadek naruszenia lub ujawnienia

ochrony danych osobowych oraz sporządza raport, który niezwłocznie przekazuje Administratorowi. Raport powinien zawierać w szczególności:

1) wskazanie osoby powiadamiającej oraz innych osób zaangażowanych lub odpytywanych w związku z naruszeniem lub ujawnieniem ochrony danych osobowych;
2) określenie czasu i miejsca naruszenia/ujawnienia i powiadomienia o tym fakcie;
3) określenie okoliczności towarzyszących i rodzaju naruszenia/ujawnienia;
4) wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania;
5) wstępną ocenę przyczyn wystąpienia naruszenia/ujawnienia;
6) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

VI. POSTANOWIENIA KOŃCOWE.

Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu, mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która po stwierdzeniu naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia, nie powiadomiła o tym fakcie Inspektora Ochrony Danych Osobowych.

Polityka Bezpieczeństwa Danych Osobowych zatwierdzona uchwałą Nr …./……/23 z dnia …… 2023r.

…….. (data)

…….. (Podpis Zarządu)

VII. ZAŁĄCZNIKI

Zal. 1) Wzór oświadczenia o zapoznaniu się z „Polityką bezpieczeństwa”.

Kartuzy, dnia ….....

Imię i nazwisko

……

Stanowisko

……

OŚWIADCZENIE

Niniejszym, działając w imieniu własnym oświadczam, iż:

1. Znana jest mi treść ustawy z dnia 10.05.2018r. o ochronie danych osobowych oraz treść „Polityki bezpieczeństwa danych osobowych w Spółdzielni Mieszkaniowej Kaszuby w Kartuzach i wydanych na jej podstawie:

1) *„Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Spółdzielni Mieszkaniowej Kaszuby w Kartuzach”;*
2) *„Instrukcja w sprawie zasad postępowania przy przetwarzaniu danych osobowych w Spółdzielni Mieszkaniowej „Kaszuby” w Kartuzach”.*

2. Zobowiązuję się do zachowania w tajemnicy wszelkich danych osobowych oraz sposobów ich zabezpieczenia, do których dostęp uzyskałem/łam w trakcie wykonywania obowiązków służbowych zarówno w czasie trwania stosunku pracy jak i po jego ustaniu,

3. Zobowiązuje się chronić dane osobowe przed dostępem do nich osób nieupoważnionych, zabezpieczać je przed zniszczeniem oraz nielegalnym ujawnieniem.

……..

(czytelny podpis)

Zał. 2) Wzór upoważnienia do przetwarzania danych.

Data nadania upoważnienia: ….....

Upoważnienie do przetwarzania danych osobowych

1. Na podstawie Rozporządzenia Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych upoważniam Pana/Panią: …..... zatrudnionego/ną na stanowisku: …..... w Spółdzielni Mieszkaniowej Kaszuby w Kartuzach, do przetwarzania danych osobowych, w celach związanych z zajmowanym stanowiskiem, w następującym zakresie: …..... .....

….....

….....

….....

(należy wskazać zbiór danych oraz zakres i formę przetwarzanych danych osobowych)

2. Identyfikator w systemie informatycznym: ….....

3. Okres na jaki wydano upoważnienie: ….....

…..... .....

(pieczęć i podpis Administratora)

Zał. 3) Wzór oświadczenia o zachowaniu w poufności uzyskanych danych osobowych oraz sposobów ich zabezpieczenia.

Kartuzy, dnia ….....

Imię i nazwisko

……

Adres

……

……

OŚWIADCZENIE

Zobowiązuję się niniejszym do zachowania w tajemnicy wszelkich danych osobowych oraz sposobów ich zabezpieczenia, do których dostęp uzyskałem/łam w związku z ….....…..... oraz do przestrzegania przepisów 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) oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, a także wewnętrznych uregulowań dotyczących ochrony danych osobowych, obowiązujących w Spółdzielni Mieszkaniowej Kaszuby w Kartuzach.

……..

(czytelny podpis)

Zał. 4) Wzór rejestru czynności przetwarzania danych osobowych

			DANE KONTAKTOWE
NAZWA ADMINISTRATORA			
NAZWA PRZEDSTAWICIELA			
IMIĘ I NAZWISKO INSPEKTORA			

Kategorie osób, których dane dotyczą	Kategorie danych osobowych	Kategorie odbiorców, którym dane ujawniono lub zostaną ujawnione	opis technicznych i organizacyjnych środków bezpieczeństwa	Cel Przetwarzania	Planowane terminy usunięcia danych
Np. klienci	*Np. imię, nazwisko, nr PESEL, adres zamieszkania, itd*	*Np. firma pocztowa*	*Np. zabezpieczenie loginem i hasłem*	*np. przeprowadzenie przeglądów technicznych*	*Np. 5 lat od sprzedaży lokalu mieszkalnego*
Np. kontrahenci	*Np. imię, nazwisko, nr PESEL, NIP, adres e-mail, itd*	*Np. kurier,*	*Np. zabezpieczenie sprzętowe USB*	*np. badania lekarskie pracowników*	*Np. 5 lat od rozwiązania umowy z uwagi na brzmienie art. 74 ust. 2 pkt 4 Ustawy o rachunkowości*
Np. kandydaci do pracy	*Np. imię, nazwisko, nr PESEL, nr NIP, adres zamieszkania, itd*	*Np. dane nie są ujawniane odbiorcom,*	*Np. zabezpieczenie loginem i hasłem*	*np. rekrutacja*	*Np. 1 miesiąc od zakończenia rekrutacji, gdy kandydat nie przejdzie jej pomyślnie*

Zał. 5) Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych.

Lp.	Imię	Nazwisko	Stanowisko	Zakres	Data nadania	Data ustania	Identyfikator w systemie informatycznym
1.							
2.							

Zał. 6) Wzór oświadczenia o wyrażeniu zgody na przetwarzanie danych osobowych w tym danych wrażliwych

Oświadczenie o wyrażeniu zgody na przetwarzanie danych osobowych w tym danych wrażliwych

Niniejszym oświadczam, że świadomy(a) moich praw wynikających z 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) oraz Ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych, wyrażam zgodę na przetwarzanie moich danych osobowych w tym danych wrażliwych przez Spółdzielni Mieszkaniowej

Kaszuby w Kartuzach, w zakresie w jakim wynikają one z treści mojego wniosku do Zarządu/Rady Nadzorczej Spółdzielni z dnia ……r.

…….. ……

(miejscowość, data) (podpis)