POLITYKA BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH W ZIELONOGÓRSKIEJ SPÓŁDZIELNI MIESZKANIOWEJ

I. Podstawa prawna

1. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.

2. 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) dalej RODO.

II. Przeznaczenie i definicje

Polityka Bezpieczeństwa określa tryb i zasady ochrony danych osobowych przetwarzanych w Zielonogórskiej Spółdzielni Mieszkaniowej.

Ilekroć w polityce bezpieczeństwa jest mowa o:

- **administratorze** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych, Administratorem danych osobowych członków Spółdzielni, osób niebędących członkami Spółdzielni i jej pracowników jest Zielonogórska Spółdzielnia Mieszkaniowa z siedzibą w Zielonej Górze, ul. Morelowa 34,
- **inspektor ochrony danych** – osoba wyznaczona przez administratora, nadzorująca przestrzeganie zasad i wymogów ochrony danych osobowych. Administrator wyznaczył inspektora ochrony danych w Zielonogórskiej Spółdzielni Mieszkaniowej.
  Dane kontaktowe: Inspektor Ochrony Danych: e-mail: iod@zielonogorska-sm.pl ; listownie: ul. Morelowa 34, 65-434 Zielona Góra,
- **systemie informatycznym** - to system przetwarzania, przechowywania i dystrybucji informacji w formie cyfrowej wraz ze związanymi z nim ludźmi oraz zasobami technicznymi i finansowymi,
- **systemie tradycyjnym** - to zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji, wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze,
- **zabezpieczeniu danych w systemie informatycznym** - wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym dostępem do nich i ich przetwarzaniem,
- **usuwaniu danych** - to trwałe i nieodwracalne zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ich odtworzenie oraz ustalenie tożsamości osoby, której dane dotyczą,
- **administratorze systemu informatycznego** - osobę/podmiot upoważnioną przez administratora do realizacji zadań związanych z zarządzaniem systemem informatycznym,
- **użytkowniku systemu informatycznego** - upoważnionego przez administratora pracownika do przetwarzania danych osobowych w systemie informatycznym.

III. Cele

Celem opracowania polityki bezpieczeństwa jest ochrona przed niepowołanym dostępem do:

a) systemu informatycznego oraz informacji przechowywanych oraz przetwarzanych z jego

wykorzystaniem;

b) informacji zgromadzonych, przetwarzanych w ramach systemu tradycyjnego.

Niniejsze opracowanie określa politykę bezpieczeństwa w zakresie przetwarzania danych osobowych przez pracowników Zielonogórskiej Spółdzielni Mieszkaniowej, a w szczególności Kierowników komórek organizacyjnych i pracowników samodzielnych oraz administratora systemów informatycznych.

Dane osobowe w Zielonogórskiej Spółdzielni Mieszkaniowej są gromadzone, przechowywane, edytowane, archiwizowane w kartotekach, skorowidzach, księgach, wykazach, rejestrach oraz w innych zbiorach ewidencyjnych poszczególnych komórek organizacyjnych Spółdzielni na dokumentach papierowych, jak również w systemach informacyjnych na elektronicznych nośnikach informacji.

Polityka bezpieczeństwa wprowadza regulacje w zakresie organizacji procesu przetwarzania i odnosi się swoją treścią do informacji:

1) w formie papierowej - przetwarzanej w ramach systemu tradycyjnego;
2) w formie elektronicznej - przetwarzanej w ramach systemu informatycznego.

Bezpośredni nadzór nad przetwarzaniem danych osobowych sprawują kierownicy komórek organizacyjnych w przypadku stanowisk samodzielnych pracownicy samodzielni.

Z zapisami w polityce bezpieczeństwa obowiązkowo są zapoznawani wszyscy użytkownicy systemów informatycznych i tradycyjnych.

Do informacji przechowywanych w systemach informatycznych jak i dokumentów tradycyjnych mają dostęp jedynie upoważnieni pracownicy Zielonogórskiej Spółdzielni Mieszkaniowej. Wszyscy pracownicy zobowiązani są do zachowania tych danych w tajemnicy. Każdy użytkownik systemu informatycznego zobowiązany jest zapamiętać swój identyfikator i hasło i nie udostępniać go innym osobom. Użytkownik systemu informatycznego powinien pamiętać o wylogowaniu się po zakończeniu korzystania z usług systemów informatycznych.

Politykę bezpieczeństwa stosuje się w szczególności do:

1) danych osobowych przetwarzanych w systemie informatycznym,
2) wszystkich informacji dotyczących danych ,
3) informacji dotyczących zabezpieczenia danych osobowych, w systemach przetwarzania danych osobowych,
4) rejestru pracowników mających upoważnienia administratora do przetwarzania danych osobowych,
5) innych dokumentów zawierających dane osobowe.

IV. Administracja i organizacja bezpieczeństwa

1. Za bezpieczeństwo danych osobowych przetwarzanych w systemach przetwarzania danych osobowych odpowiada administrator. Kierownicy komórek organizacyjnych, pracownicy samodzielni obowiązani są zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, a w szczególności powinni zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą uszkodzeniem lub zniszczeniem.

2. Inspektor Ochrony Danych sprawuje nadzór nad ochroną danych osobowych i zapewnienie zgodności przetwarzania z przepisami dotyczącymi ochrony danych osobowych, a w szczególności IOD:

a) zachowuje w tajemnicy lub poufności szczegóły wykonywanych zadań,
b) informuje administratora, podmiot przetwarzający oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich w związku z ochroną danych osobowych,
c) monitoruje przestrzeganie przepisów o ochronie danych, prowadzi działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty,
d) współpracuje z organem nadzorczym,
e) udziela informacji osobom, których dane dotyczą informacji zgodnie z przysługującymi im prawami,
f) pełni funkcję punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych (w tym z uprzednimi konsultacjami zgodnie z art. 36),
g) pełni rolę punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO,
h) prowadzi rejestr czynności przetwarzania danych osobowych.

3. Administrator systemu informatycznego wykonuje wszystkie prace niezbędne do efektywnego oraz bezpiecznego zarządzania systemem informatycznym, a w szczególności:
   a) odpowiada za bezpieczeństwo systemu informatycznego i zapewnia ciągłość działania systemu informatycznego oraz baz danych,
   b) zobowiązuje i bieżąco kontroluje stosowanie się użytkowników do obowiązujących procedur,
   c) utrzymuje i aktualizuje listę autoryzowanych użytkowników systemu informatycznego,
   d) optymalizację wydajności systemu informatycznego, instalacje i konfiguracje sprzętu sieciowego i serwerowego,
   e) instalacje i konfiguracje oprogramowania systemowego, sieciowego,
   f) konfigurację i administrowanie oprogramowaniem systemowym, sieciowym oraz zabezpieczającym dane chronione przed nieupoważnionym dostępem,
   g) nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych,
   h) zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego,
   i) zarządzanie kopiami awaryjnymi danych osobowych oraz zasobów umożliwiających ich przetwarzanie,
   j) przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,
   k) przyznawanie na wniosek administratora lub inspektora ochrony danych ściśle określonych praw dostępu do informacji w danym systemie,
   l) wnioskowanie do administratora lub inspektora ochrony danych w sprawie zmian lub usprawnienia procedur bezpieczeństwa i standardów zabezpieczeń,
   m) zarządzanie licencjami, procedurami ich dotyczącymi,
   n) prowadzenie profilaktyki antywirusowej.

4. Osoby upoważnione do przetwarzania danych osobowych mają obowiązek:
   - przetwarzać je zgodnie z przepisami,
   - nie udostępniać ich oraz uniemożliwiać dostęp do nich osobom nieupoważnionym,
   - zabezpieczać je przed zniszczeniem.

5. Użytkownik systemu informatycznego wykonuje wszystkie prace niezbędne do efektywnej oraz bezpiecznej pracy na stanowisku pracy również z wykorzystaniem stacji roboczej. Jest odpowiedzialny przed IOD za nadzór i utrzymanie niezbędnych warunków bezpieczeństwa w szczególności do przestrzegania procedur dostępu do systemu i ochrony danych osobowych.

6. Zasady przetwarzania danych w systemie informatycznym określone są w „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Zielonogórskiej Spółdzielni Mieszkaniowej".

V. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

1. Dane osobowe są gromadzone, przechowywane i przetwarzane w kartotekach, skorowidzach, księgach, wykazach, rejestrach oraz w innych zbiorach ewidencyjnych poszczególnych komórek organizacyjnych Zielonogórskiej Spółdzielni Mieszkaniowej w postaci dokumentów papierowych. Do przetwarzania zbiorów danych osobowych w systemie informatycznym Spółdzielni, stosowane są pakiety biurowe lub specjalizowane aplikacje (programy).

2. Dane osobowe w postaci papierowej upoważnieni pracownicy przechowują w obszarze przetwarzania danych w szafach zamykanych na klucz.

3. Do stosowania zasad określonych przez Politykę bezpieczeństwa oraz inne z nią związane dokumenty zobowiązani są wszyscy pracownicy, stażyści, praktykanci oraz inne osoby mające dostęp do danych osobowych podlegających ochronie.

VI. Opis kategorii osób, których dane dotyczą oraz kategorii danych osobowych

Zbiory danych osobowych w Zielonogórskiej Spółdzielni Mieszkaniowej podzielone są na zestawienie zbiorów przetwarzanych w Spółdzielni, które gromadzi się, przechowuje i przetwarza tradycyjnie w postaci papierowej, jak również w systemie informatycznym.

VII. Sposób przepływu danych pomiędzy poszczególnymi systemami

1. Obieg dokumentów zawierających dane osobowe, pomiędzy komórkami organizacyjnymi Zielonogórskiej Spółdzielni Mieszkaniowej, winien odbywać się w sposób zapewniający pełną ochronę przed ujawnieniem zawartych w tych dokumentach danych (informacji).

2. Przekazywanie informacji (danych) w systemie informatycznym poza sieć wewnętrzną Zielonogórskiej Spółdzielni Mieszkaniowej odbywa się w sposób zapewniający pełną ochronę.

VIII. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1. Dostęp do danych wprowadzanych przez użytkowników systemów informatycznych mają jedynie upoważnieni pracownicy oraz administrator systemu zapewniający jego prawidłową eksploatację. Wszyscy pracownicy, będący użytkownikami systemu zobowiązani są do zachowania tych danych w tajemnicy.

2. Ochronie podlegają dane osobowe gromadzone i przetwarzane w kartotekach, skorowidzach, księgach, wykazach, rejestrach i w innych zbiorach ewidencyjnych oraz w urządzeniach i systemach informatycznych Zielonogórskiej Spółdzielni Mieszkaniowej.

3. Pomieszczenia, w których przetwarza się dane osobowe powinny być fizycznie zabezpieczone przed dostępem osób nieupoważnionych, to znaczy posiadać odpowiednie zamki do drzwi, zabezpieczenia w oknach (w szczególności na parterze) oraz być wyposażone w środki ochrony p.poż.

4. Dokumenty i nośniki informacji, zawierające dane osobowe powinny być zabezpieczone przed dostępem osób nieupoważnionych do przetwarzania danych. Jeśli nie są aktualnie używane powinny być przechowywane w szafach, biurkach lub innych przeznaczonych do tego celu urządzeniach biurowych, posiadających odpowiednie zabezpieczenie - zamki.

IX. Udostępnianie posiadanych danych w zbiorze danych osobowych

1. Do udostępniania posiadanych w zbiorze danych osobowych upoważnionych jest administrator lub pracownik posiadający wymagane upoważnienie.

2. W przypadku udostępnienia danych osobowych w celach innych niż włączenie do zbioru, administrator udostępnia posiadane w zbiorze dane osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa lub na podstawie odpowiednich umów powierzenia.

X. Bezpieczeństwo fizyczne, sprzętu i oprogramowania

1. Pomieszczenia, w których znajdują się stanowiska komputerowe są: zamknięte, jeśli nikt w nich nie przebywa; wyposażone w szafy, biurka umożliwiające przechowywanie dokumentów.

2. Sprzęt i oprogramowanie, mają ścisły związek z bezpieczeństwem systemu i sieci teleinformatycznej. Dlatego, powinny być przestrzegane procedury bezpieczeństwa odnoszące się do ich elementów.

3. Sieć teleinformatyczna jest organizacyjnym i technicznym połączeniem systemów teleinformatycznych wraz z łączącymi je urządzeniami i liniami telekomunikacyjnymi. Niedopuszczalne jest samowolne przemieszczanie lub zmiana konfiguracji stacji roboczej bez wiedzy kierownika komórki organizacyjnej.

4. Nie zezwala się na korzystanie z jakiegokolwiek nowego oprogramowania bez zgody Zarządu Spółdzielni. Dodatkowe oprogramowanie może być instalowane wyłącznie po uzyskaniu takiej zgody. Używanie oprogramowania prywatnego w sieci jest kategorycznie zabronione. Na stacjach roboczych powinno być zainstalowane jedynie niezbędne oprogramowanie.

5. W przypadku uszkodzenia nośnika magnetycznego zawierającego dane osobowe należy komisyjnie dokonać jego zniszczenia.

6. Serwer systemu, krytyczne urządzenia sieciowe oraz poszczególne stacje robocze powinny być zabezpieczone urządzeniami podtrzymującymi zasilanie (UPS), co umożliwia funkcjonowanie systemu w przypadku awarii zasilania.

7. W celu zabezpieczenia ciągłości pracy, informacja przechowywana i przetwarzana w systemie podlega codziennej, przyrostowej archiwizacji oraz pełnej archiwizacji. Kopie archiwalne danych są wykonywane na nośnikach magnetooptycznych i przechowywane przez Zielonogórską Spółdzielnię Mieszkaniową. Użycie kopii zapasowych następuje w przypadku odtworzenia systemu po awarii.

XI. Zabezpieczenia organizacyjne

1. Opracowano i wdrożono Politykę bezpieczeństwa przetwarzania danych osobowych.
2. Sporządzono i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Zielonogórskiej Spółdzielni Mieszkaniowej.
3. Wyznaczono inspektora ochrony danych.
4. Do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora.
5. Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego.
6. Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy.
7. Przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych.
8. Przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych.
9. Dokumenty i nośniki informacji zawierające dane osobowe, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonuje się takiej ich modyfikacji, która nie pozwoli na odtworzenie ich treści.

XII. Zabezpieczenia techniczne

1. Wewnętrzną sieć komputerową zabezpieczono poprzez odseparowanie od sieci publicznej za pomocą Firewall.
2. Stanowiska komputerowe wyposażono w indywidualną ochronę antywirusową.
3. Komputery zabezpieczono przed możliwością użytkowania przez osoby nieuprawnione do przetwarzania danych osobowych, za pomocą indywidualnego identyfikatora użytkowania i cykliczne wymuszanie zmiany hasła.
4. Dostęp do sieci wewnętrznej Zielonogórskiej Spółdzielni Mieszkaniowej możliwy jest tylko dla ściśle kontrolowanej listy urządzeń na poziomie urządzeń sieciowych.

XIII. Środki ochrony fizycznej

1. Obszar, na którym przetwarzane są dane osobowe, poza godzinami pracy, chroniony jest alarmem.
2. Obszar, na którym przetwarzane są dane osobowe objęty jest całodobowym monitoringiem.
3. Urządzenia służące do przetwarzania danych osobowych umieszczone są w zamykanych pomieszczeniach.
4. Dokumenty i nośniki informacji zawierające dane osobowe przechowywane są w zamykanych na klucz szafach.

XIV. Polityka antywirusowa

W zakresie ochrony antywirusowej wprowadza się następujące zalecenia:

a) nie należy używać oprogramowania na stacjach roboczych innego niż zaleca administrator systemu,
b) zabrania się instalowania oprogramowania typu freeware czy shareware,
c) regularnie uaktualniać bazę wirusów zainstalowanego oprogramowania antywirusowego,
d) przed użyciem nośnika danych sprawdzić czy nie jest zainfekowany wirusem komputerowym.

XV. Postanowienia końcowe

1. „Polityka bezpieczeństwa ochrony danych osobowych w Zielonogórskiej Spółdzielni Mieszkaniowej" zatwierdzona Uchwałą Zarządu Zielonogórskiej Spółdzielni Mieszkaniowej Nr 19/2018 z dnia 25.05.2018 r. i obowiązuje od dnia uchwalenia.
2. Traci moc Polityka z dnia 29.01.2014 r. wraz z załącznikami.

Zielonogorska
Spółdzielnia Mieszkaniowa
ul. Morelowa 34
65-434 Zielona Góra
tel. cent. (68) 454 69 00, tel./fax (68) 327 05 84
www.zielonogorska-sm.pl

Z-CA PREZESA
ds. techniczno - eksploatacyjnych
Tomasz Kasprzyszak

PREZES ZARZĄDU
Dariusz Maćkowiak

Załączniki:

1. Ewidencja osób upoważnionych do przetwarzania danych osobowych – wzór.
2. Wykaz budynków, w których przetwarzane są dane osobowe - wzór.
3. Rejestr czynności przetwarzania danych osobowych – wzór.

Załączniki Nr 1

Ewidencja osób upoważnionych do przetwarzania danych osobowych w Zielonogórskiej Spółdzielni Mieszkaniowej – wzór

Lp	Nazwisko	Imię	Stanowisko służbowe	Nazwa komórki organizacyjnej	Lokalizacja pomieszczeń			Data		Nr upoważnienia
					lokalizacja	kondygnacja	numer pokoju	nadania upoważ.	ustania upoważ.	

Załącznik Nr 2

Wykaz budynków, w których przetwarzane są dane osobowe - wzór.

1. .....
2. .....
3. .....

Załącznik Nr 3

Rejestr czynności przetwarzania danych osobowych - wzór.

Nazwa administratora danych: .....

Dane kontaktowe administratora danych: .....

Dane kontaktowe przedstawiciela administratora danych: .....

Dane kontaktowe współadministratorów: .....

Dane kontaktowe Inspektora Ochrony Danych: .....

L.p.	Nazwa zbioru danych osobowych	Cel przetwarzania danych	Opis kategorii osób, których dane dotyczą oraz kategorii danych osobowych	Kategorie odbiorców, którym dane zostały lub zostaną ujawnione	Kategorie odbiorców, którym dane zostały lub zostaną ujawnione w państwach trzecich	Kategorie odbiorców, którym dane zostały lub zostaną ujawnione w organizacjach międzynarodowych	Planowane terminy usunięcia poszczególnych kategorii danych	Opis technicznych i organizacyjnych środków bezpieczeństwa