INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W ZIELONOGÓRSKIEJ SPÓŁDZIELNI MIESZKANIOWEJ

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).

SPIS TREŚCI

I. Postanowienia ogólne

Instrukcja zarządzania systemem informatycznym nakłada na administratora danych osobowych następujące obowiązki:

1) zapewnienie bezpieczeństwa i poufności danych, w tym zabezpieczenie ich przed ujawnieniem,
2) zabezpieczenie danych przed udostępnieniem osobom nieupoważnionym (nieuprawnionym pozyskaniem),
3) zabezpieczenie przed utratą danych,
4) zabezpieczenie przed uszkodzeniem lub zniszczeniem danych oraz przed ich nielegalną modyfikacją.

Ochronie podlegają dane osobowe niezależnie od formy przechowywania, sprzęt komputerowy, systemy operacyjne i informatyczne oraz pomieszczenia, w których odbywa się proces przetwarzania.

Instrukcja określa ramowe zasady właściwego zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne, odpowiednie do zagrożeń i kategorii danych objętych ochroną.

II. Przeznaczenie, definicje

Instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Zielonogórskiej Spółdzielni Mieszkaniowej w Zielonej Górze, zwaną dalej Instrukcją – określa sposób zarządzania oraz zasady administrowania systemem informatycznym służącym do przetwarzania danych osobowych członków Spółdzielni, osób niebędących członkami Spółdzielni i jej pracowników.

Ilekroć w instrukcji jest mowa o:

1) **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,
2) **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,*
3) **danych osobowych** – każdą informację dotyczącą osoby fizycznej, bądź osoby prawnej pozwalającą na określenie tożsamości tej osoby,
4) **zbiorze danych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony czy podzielony funkcjonalnie,
5) **przetwarzaniu danych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
6) **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,
7) **administratorze systemu informatycznego** – osoba/podmiot nadzorujący i odpowiadający za poprawną pracę powierzonego mu sprzętu sieciowego oraz systemu operacyjnego w Spółdzielni, w tym w szczególności:
   - mającą prawo do zmiany uprawnień wszystkich użytkowników,
   - za pomocą platformy zarządzania dysponują bezpośrednio wszystkimi zasobami podległej mu sieci,
   - pełnią kontrole nad dostępem użytkowników, do systemów,
   - podejmującą samodzielnie lub na polecenie administratora bezpieczeństwa informacji odpowiednie działania w wypadku naruszeń w systemie zabezpieczeń,
8) **użytkownikach systemów** – osoby upoważnione do przetwarzania danych osobowych w systemie informatycznym,
9) **obszarze kontrolowanym** – obszar znajdujący się pod ochroną, o ograniczonym dostępie osób nieautoryzowanych, w którym odbywa się przetwarzanie danych, w tym danych osobowych.

Niniejsza Instrukcja zarządzania systemem informatycznym określa:

a) poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym;
b) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym;

c) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;
d) sposób przydziału haseł i loginów dla użytkowników;
e) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
f) metoda i częstotliwość tworzenia kopii;
g) metoda i częstotliwość sprawdzania obecności wirusów komputerowych oraz metoda ich usuwania;
h) sposób, miejsce i okres przechowywania:
   - elektronicznych nośników informacji zawierających dane osobowe,
   - kopii zapasowych;
i) sposób dokonywania przeglądów i konserwacji systemów i zbioru danych osobowych;
j) sposób postępowania w zakresie komunikacji w sieci komputerowej;
k) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

III. Zasady prowadzenia ewidencji pracowników Spółdzielni zatrudnionych przy przetwarzaniu danych osobowych

1. Inspektor ochrony danych prowadzi ewidencję wszystkich pracowników Spółdzielni zatrudnionych przy przetwarzaniu danych osobowych.

2. Powyższa ewidencja uwzględnia:
   – nazwisko i imię pracownika,
   – stanowisko służbowe,
   – nazwa komórki organizacyjnej,
   – lokalizacja pomieszczeń,
   – data nadania upoważnienia,
   – data ustania upoważnienia,
   – numer upoważnienia.
   – systemy – programy informatyczne, do których wydane zostało upoważnienie.

3. Jakakolwiek zmiana informacji wyszczególnionej w ewidencji podlega natychmiastowemu odnotowaniu.

IV. Zasady rejestrowania i wyrejestrowania użytkowników systemu informatycznego, zakres odpowiedzialności administratora systemu

1. Rejestracji i wyrejestrowania użytkownika systemu informatycznego dokonuje upoważniona przez IOD osoba/podmiot ujęta/y w ewidencji osób uprawnionych do przetwarzania danych osobowych zwana Administratorem Systemu Informatycznego.

2. Za zarejestrowanie i wyrejestrowanie użytkownika odpowiedzialna jest Zielonogórska Spółdzielnia Mieszkaniowa a w jej imieniu Zarząd Spółdzielni.

3. Każdy użytkownik upoważniony do pracy w systemie informatycznym, w którym przetwarzane są dane osobowe, winien posiadać indywidualny, imienny identyfikator i hasło dostępu.

4. Rozwiązanie stosunku pracy, bądź zmiana zakresu obowiązków powoduje utratę dostępu do przetwarzania danych i natychmiastowe wyrejestrowanie użytkownika z systemu oraz wykreślenie z ewidencji.

V. Zasady dopuszczania pracowników Spółdzielni do eksploatacji systemów informatycznych przetwarzających zbiory danych osobowych

Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do zbierania lub przetwarzania danych osobowych, mogą być dopuszczeni wyłącznie pracownicy posiadający aktualne, ważne upoważnienie wydane przez Administratora danych.
IOD zapoznaje pracowników z przepisami o ochronie danych osobowych oraz wykaz akt i wiadomości stanowiących tajemnicę służbową (w zakresie danych osobowych).

VI. Zasady tworzenia i posługiwania się hasłami dostępu do systemów informatycznych

1. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym użytkownik może mieć wyłącznie po podaniu identyfikatora i hasła.

2. Hasło powinno zawierać od 5 do 10 znaków, w tym litery duże i małe oraz znaki specjalne i cyfry. Zmiana haseł następuje, co 30 dni.

3. Użytkownicy nie mogą korzystać z innych identyfikatorów i haseł niż te, do których są upoważnieni oraz nie mogą nadanych im użytkownika i hasła przekazywać innym osobom z wewnątrz Spółdzielni jak i spoza niej.

4. Identyfikator użytkownika nie może być zmieniany, a po wyrejestrowaniu Użytkownika z systemu informatycznego nie może być przydzielony innej osobie.

5. Szczególnym zasadom poufności i ochronie podlegają hasła administratorów systemu.

VII. Procedury rozpoczęcia, kontynuowania i zakończenia pracy z systemem informatycznym

1. Użytkownik rozpoczynający pracę zobowiązany jest przestrzegać procedur, które mają na celu sprawdzenie zabezpieczenia pomieszczeń, w których przetwarzane są dane osobowe, swojego stanowiska pracy oraz stanu sprzętu komputerowego.

2. Krótkotrwałe przerwy w pracy (bez opuszczenia stanowiska pracy) nie wymagają zamykania aplikacji, modułu.

3. Przed opuszczeniem stanowiska pracy, użytkownik obowiązany jest zamknąć aplikację, moduł i wylogować się z pracy w sieci. Dopilnować, aby na ekranie nie były wyświetlane dane osobowe.

4. Przy czasowym opuszczaniu stanowiska należy ustawić ręcznie blokadę ekranu komputera z koniecznością ponownego podania identyfikatora i hasła.

5. Pomieszczenia, w których przetwarzane są dane osobowe po zakończeniu pracy zamyka się.

VIII. Procedury tworzenia kopii zapasowych zbiorów danych osobowych oraz programów i urządzeń programowych służących do ich przetwarzania.

- Zasady tworzenia kopii.

1. Kopie zapasowe z każdej aplikacji powinny być sporządzane na dyskach magnetycznych, w cyklu miesięcznym.

2. Dodatkowo należy sporządzać kopie robocze roczne, bilansowe.

- Zasady przechowywania nośników informacji ze zbiorami danych (w tym danych osobowych) oraz kopii bezpieczeństwa.

1. Nośniki elektroniczne przeznaczone do przechowywania danych osobowych powinny się charakteryzować odpowiednią trwałością zapisu, zależną od planowanego okresu przechowywania na nich danych.

2. Czas przechowywania kopii zbiorów ustala się na:
   - bieżąca kopia zapasowa - 1 miesiąc,
   - kopia roczna - ostatni dzień okresu bilansowego – 10 lat.

3. Miejsca przechowywania kopii bezpieczeństwa muszą podlegać szczególnej ochronie.

4. Zabrania się wynoszenia jakichkolwiek nagranych nośników zawierających dane osobowe z miejsca pracy.

IX. Zasady niszczenia i sposoby dokumentowania procesu niszczenia nośników informacji zawierających dane osobowe

1. Jeżeli usunięcie danych osobowych z nośników magnetycznych lub optycznych nie jest możliwe wówczas nośniki takie zostają zniszczone w sposób uniemożliwiający ich odczytanie.

2. Nośniki papierowe (wydruki) nieprzeznaczone do ponownego użytku oraz niearchiwizowane powinny być natychmiast niszczone.

X. Określenie zasad zabezpieczenia oraz wykonywania przeglądów i konserwacji systemów służących do przetwarzania danych

1. Na wszystkich komputerach zainstalowanych w Spółdzielni może być instalowane wyłącznie legalne oprogramowanie posiadające licencję, certyfikat legalności itp.

2. Zaleca się systematyczny przegląd stanowisk komputerowych, serwerów i urządzeń sieciowych pod kątem:

   a) właściwości i legalności zainstalowanego oprogramowania. Potrzebę instalacji jakiegokolwiek oprogramowania należy zgłosić i uzgodnić z Działem Organizacyjno – Administracyjnym. Realizacja zaplanowanych, w tym zakresie czynności nastąpi po uzyskaniu zgody Zarządu Spółdzielni a samowolne pobieranie i instalowanie oprogramowania przez użytkowników jest surowo zabronione,
   b) optymalizacji konfiguracji i poziomu bezpieczeństwa danych osobowych, użytkowników, systemów operacyjnych i sieci.

3. Na stacjach roboczych z dostępem do Internetu należy zainstalować oprogramowanie antywirusowe, które oprócz ochrony przed złośliwym oprogramowaniem stwarza dodatkową funkcjonalność kontroli bezpieczeństwa przeglądania stron internetowych i poczty elektronicznej.

XI. Zabezpieczenie przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

1. Dla potrzeb systemu informatycznego w Spółdzielni stosowane jest zabezpieczenie antywirusowe. W zakres jego funkcjonalności wchodzą m.in.: ochrona przed złośliwym

oprogramowaniem, ochrona poczty, skanowanie ruchu sieciowego, ochrona systemu plików, kontrola zmian w systemie plików, monitorowanie procesów w pamięci, monitorowanie i zapobieganie zmianom w rejestrze systemowym.

2. Aktualizacja oprogramowania oraz definicji wirusów odbywa w sposób automatyczny. Wszystkie wykryte zagrożenia bezpieczeństwa rejestrowane są w centralnej konsoli z natychmiastowym powiadomieniem Administratora Systemu Informatycznego pocztą elektroniczną.

3. Do usuwania złośliwego oprogramowania należy używać wyłącznie programów antywirusowych, pozostających w dyspozycji Spółdzielni.

4. Urządzenia i nośniki zawierające dane osobowe przekazywane poza obszar, w którym są one przetwarzane, zabezpiecza się w sposób zapewniający poufność i integralność danych.

5. Wysyłane przy użyciu poczty elektronicznej dokumenty z danymi osobowymi realizowane jest w taki sposób iż odbiorca otrzymuje jedynie bezpieczny link do dokumentu umieszczonego w systemie chmurowym Spółdzielni. Dodatkowo plik taki jest zabezpieczony poprzez zastosowanie programu kompresującego, szyfrującego dane oraz zabezpieczającego plik hasłem. Nadawca przekazuje odbiorcy e-maila hasło w inny sposób, aniżeli poprzez pocztę elektroniczną, np. smsem, listem, podczas rozmowy telefonicznej, bądź osobiście.

XII. Postępowanie w zakresie komunikacji sieciowej

1. Przeglądarka internetowa powinna mieć ustawione opcje tak, by nie zapamiętywała nazwy użytkownika oraz hasła.

2. Komunikacja w sieci komputerowej Spółdzielni dozwolona jest wyłącznie przy użyciu ściśle kontrolowanej listy urządzeń, będących własnością Spółdzielni po odpowiednim zalogowaniu się za pomocą indywidualnego hasła i identyfikatora użytkownika.

3. Dostęp zdalny do sieci komputerowej Spółdzielni możliwy jest jedynie po uprzednim wypełnieniu oraz zatwierdzeniu przez Spółdzielnię stosownego formularza i nadania indywidualnych parametrów i procedury dostępu zdalnego.

XIII. Postanowienia końcowe

1. Każda osoba wpisana do ewidencji zobowiązana jest do zapoznania się z:
   - Regulaminem ochrony danych osobowych w Zielonogórskiej Spółdzielni Mieszkaniowej w Zielonej Górze,
   - Polityką bezpieczeństwa danych osobowych w Zielonogórskiej Spółdzielni Mieszkaniowej w Zielonej Górze,
   - niniejszą Instrukcją.

2. Wszelkie zagadnienia dotyczące ochrony danych osobowych nie ujęte w niniejszej Instrukcji należy rozpatrywać zgodnie z „Regulaminem ochrony danych osobowych w Zielonogórskiej Spółdzielni Mieszkaniowej w Zielonej Górze" i „Polityką bezpieczeństwa danych osobowych w Zielonogórskiej Spółdzielni Mieszkaniowej" z uwzględnieniem późniejszych zmian i uzupełnień.

3. „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Zielonogórskiej Spółdzielni Mieszkaniowej" zatwierdzona Uchwałą Zarządu Zielonogórskiej Spółdzielni Mieszkaniowej Nr 20/2018 z dnia 25.05.2018 r. i obowiązuje od dnia uchwalenia.

4. Traci moc Instrukcja z dnia 29.01.2014 r. wraz z załącznikiem.

Zielonogórska
Spółdzielnia Mieszkaniowa
ul. Morelowa 34
65-434 Zielona Góra
Regon 000493439, NIP 929-011-20-82
www.zielonogorska-sm.pl

Z-CA PREZESA
ds. techniczno - eksploatacyjnych
Tomasz Kasprzyszak

PREZES ZARZĄDU
Dariusz Maćkowiak

Załączniki:
1. Oświadczenie o odpowiedzialności za wyposażenie.

Załącznik Nr 1

Oświadczenie o odpowiedzialności za wyposażenie

Imię i Nazwisko .....
Stanowisko służbowe .....
Nazwa komórki organizacyjnej .....

Zgodnie z art. 124 Kodeksu Pracy o odpowiedzialności za wyposażenie stanowiska pracy (sprzęt komputerowy, oprogramowanie, wraz z licencjami) pracownika, jest Pani/Pan odpowiedzialna/y za powierzone mienie Zielonogórskiej Spółdzielni Mieszkaniowej. Zobowiązuje się do nieinstalowania oprogramowania nielegalnego, nielicencjonowanego, stanowiącego naruszenie zasad bezpieczeństwa określonych w „Instrukcji Zarządzania Systemem Informatycznym w Zielonogórskiej Spółdzielni Mieszkaniowej".

.....
(data i podpis składającego oświadczenie)