Spółdzielnia Mieszkaniowa
w Sępólnie Krajeńskim
ul. T. Kościuszki 16
89-400 Sępólno Krajeńskie
tel. centr. 52 388 38 17, 52 388 21 49

Regulamin Ochrony Danych Osobowych w Spółdzielni Mieszkaniowej w Sępólnie Krajeńskim

Niniejszy regulamin stanowi wykaz podstawowych obowiązków z zakresu przestrzegania zasad ochrony danych osobowych zgodnie z przepisami Rozporządzenia Parlamentu Europejskiego i Rady (EU) 2016/679 z dnia 27 kwietnia 2016 oraz ustawy o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz. U. z 2018 poz. 1000).

- Pracowników
- Zleceniobiorców
- Pracowników podmiotów trzecich, posiadających dostęp do danych osobowych przetwarzanych przez Spółdzielnię
- Użytkowników systemów informatycznych z dostępem do danych osobowych przetwarzanych przez Spółdzielnię (hosting, poczta elektroniczna)

1. Zasady bezpiecznego użytkowania sprzętu IT, dysków, programów

1. W przypadku, gdy użytkownik przetwarzający dane osobowe korzysta ze sprzętu IT zobowiązany jest do jego zabezpieczenia przed zniszczeniem lub uszkodzeniem. Jako sprzęt IT rozumie się: komputery stacjonarne, monitory, drukarki, skanery, kserokopiarki, służbowe komputery przenośne, tablety i telefony komórkowe.
2. Użytkownik jest zobowiązany zgłosić zagubienie, utratę lub zniszczenie powierzonego mu sprzętu IT.
3. Samowolne instalowanie, otwieranie (demontaż) sprzętu IT, instalowanie dodatkowych urządzeń (np. dysków twardych, pamięci) lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.
4. Użytkownik jest zobowiązany do usuwania lub zabezpieczenie hasłem plików z nośników, do których mają dostęp i inni użytkownicy nieposiadający upoważnienia do dostępu do takich plików (np. podczas współużytkowania komputerów).
5. Użytkownik jest zobowiązany do przekazania ASI* nośników przeznaczonych do zniszczenia.
6. Użytkownicy komputerów przenośnych, na których znajdują się dane osobowe lub z dostępem do danych osobowych przez Internet zobowiązani są do stosowania zasad bezpieczeństwa.

2. Zarządzanie uprawnieniami - procedura rozpoczęcia, zawieszenia i zakończenia pracy

1. Każdy użytkownik (np. komputera stacjonarnego, komputera przenośnego, dysku sieciowego, programów w których użytkownik pracuje, poczta elektroniczna) musi posiadać swój własny indywidualny identyfikator do logowania się (login).
2. Tworzenie kont użytkowników wraz z uprawnieniami (np. komputera stacjonarnego, laptopa, dysku sieciowego, programów w których użytkownik pracuje, poczty

elektronicznej) odbywa się na polecenie przełożonych a wykonywane jest przez ASI Spółdzielni.
3. Użytkownik nie może samodzielnie zmieniać swoich uprawnień (np. zostać administratorem Windows na użytkowanym komputerze).
4. Każdy użytkownik musi posiadać indywidualny identyfikator. Zabronione jest umożliwianie innym osobom pracy na koncie innego użytkownika.
5. Zabrania się pracy wielu użytkowników na wspólnym koncie.
6. Użytkownik (np. komputera stacjonarnego, laptopa, dysku sieciowego, programów w których użytkownik pracuje, poczty elektronicznej) rozpoczyna pracę z użyciem identyfikatora i hasła.
7. Użytkownik jest zobowiązany do powiadomienia ASI Spółdzielni o próbach logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje.
8. W przypadku, gdy użytkownik podczas próby zalogowania się, zablokuje możliwość dostępu do systemu, zobowiązany jest powiadomić o tym ASI Spółdzielni.
9. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom, pracownikom innych działów) wglądu do danych wyświetlanych na monitorach – tzw. **Polityka czystego ekranu.**
10. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu (WINDOWS + L) lub wylogować się z systemu operacyjnego, użytkowanego programu.
11. Zabrania się uruchamiania jakiejkolwiek aplikacji lub programu na prośbę innej osoby, o ile nie jest ona ASI Spółdzielni. Dotyczy to zwłaszcza programów przesłanych za pomocą poczty elektronicznej lub wskazanych w formie odnośnika internetowego (link).
12. Po zakończeniu pracy, użytkownik zobowiązany jest:
13. Wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy,
14. Zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki elektroniczne, magnetyczne i optyczne, na których znajdują się dane osobowe.

3. Polityka haseł

1. Hasła powinny składać się z np. 12 znaków.
2. Hasła powinny zawierać duże, małe litery oraz cyfry lub znaki specjalne.
3. Hasła nie mogą być łatwe do odgadnięcia. Nie powinny być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion i nazwisk osób bliskich, imion zwierząt, popularnych dat, popularnych słów, typowych zestawów: 123456, abcd
4. Hasła nie powinny być ujawnianie innym osobom. Nie należy zapisywać haseł na kartkach i w notesach, nie naklejać na monitorze komputera, nie trzymać pod klawiaturą lub w szufladzie.
5. W przypadku ujawnienia hasła – należy natychmiast je zmienić.
6. Hasła muszą być zmieniane co 30 dni.
7. Jeżeli system nie wymusza zmiany haseł, użytkownik zobowiązany jest do samodzielnej zmiany hasła.
8. Użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło.
9. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.

10. Zabrania się używania w serwisach internetowych, poczcie elektronicznej, wszelkich portalach takich samych lub podobnych haseł jak w systemie komputerowym Spółdzielni.
11. Zabrania się stosowania tego samego hasła jako zabezpieczenia w dostępie do różnych systemów.
12. Zabrania się definiowania haseł, w których jeden człon pozostaje niezmienny, a drugi zmienia się według przewidywalnego wzorca (np. Anna001, Anna002, Anna003 itd.). Nie powinno się też stosować haseł, w których jeden z członów stanowi imię, nazwę lub numer miesiąca lub inny możliwy do odgadnięcia frazy.

4. Zabezpieczenie dokumentacji papierowej z danymi osobowymi

1. Upoważnieni pracownicy są zobowiązani do stosowania tzw. **„Polityki czystego biurka"**. Polega ona na zabezpieczaniu (zamykaniu) dokumentów oraz nośników np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas nieobecności pracownika w trakcie godzin pracy.
2. Upoważnieni pracownicy zobowiązani są do niszczenia dokumentów i wydruków w niszczarkach. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. w korytarzach, na kserokopiarkach, drukarkach, w pomieszczeniach konferencyjnych.
3. Zabrania się wyrzucania niezniszczonych dokumentów.

5. Zasady wynoszenia nośników z danymi poza pomieszczenia biurowe SPÓŁDZIELNI

1. Użytkownicy nie mogą wynosić na zewnątrz organizacji wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody ASI Spółdzielni. Do takich nośników zalicza się: przenośne dyski twarde, płyty CD, DVD, pamięci typu Flash (pendrive, karta pamięci).
2. Dane osobowe wynoszone poza Spółdzielnią muszą być zaszyfrowane (szyfrowane dyski, pamięci zabezpieczone hasłem).
3. Należy zapewnić bezpieczne przewożenie dokumentacji papierowej w teczkach.
4. Należy korzystać ze sprawdzonych firm kurierskich.
5. W przypadku, gdy dokumenty przewozi pracownik, zobowiązany jest do zabezpieczenia przewożonych dokumentów przed zagubieniem i kradzieżą.
6. W sytuacji przekazywania nośników z danymi osobowymi poza obszar Spółdzielni można stosować następujące zasady bezpieczeństwa:
    a. adresat powinien zostać powiadomiony o przesyłce,
    b. dane przed wysłaniem powinny zostać zaszyfrowane, a hasło podane adresatowi inną drogą,
    c. stosować bezpieczne koperty depozytowe,
    d. przesyłkę należy przesyłać przez kuriera.

6. Zasady korzystania z sieci internet

1. Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych.
2. Zabrania się kopiowania na dysk twardy komputera oraz uruchamiania jakichkolwiek

nielegalnego oprogramowania oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być pobierane tylko za każdorazową zgodą ASI Spółdzielni i tylko w uzasadnionych przypadkach.

3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.
4. Zabrania się użytkowania na stron WWW, prezentujących informacje o charakterze przestępczym, hackerskim, pornograficznym lub innym, zakazanym przez prawo (większość stron tego typu posiada "złośliwy kod", infekujące system operacyjny komputera w sposób automatyczny).
5. W ustawieniach przeglądarki stron WWW nie należy w opcjach przeglądarki włączać opcji automatycznego uzupełniania formularzy i zapamiętywania haseł.
6. W przypadku korzystania z szyfrowanego połączenia w przeglądarce stron WWW, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu strony rozpoczynającego się frazą "https:". Dla pewności należy „kliknąć" na ikonkę kłódki i sprawdzić, czy właściciel certyfikatu zabezpieczającego jest wiarygodny.
7. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania, prośby zalogowania się na stronie WWW (np. strona banku, poczty elektronicznej) lub podania identyfikatora (login), hasła, PIN, numeru karty płatniczej w formularzu strony WWW lub odesłania wyżej wymienionych pocztą elektroniczną.
8. Zabrania się samowolnego podłączania do komputerów, modemów, routerów przenośnych i stacjonarnych, telefonów komórkowych i innych urządzeń dostępowych niebędących elementem infrastruktury informatycznej Spółdzielni. Zabronione jest również łączenie się przy pomocy takich urządzeń z Internetem w chwili, gdy komputer użytkownika podłączony jest do sieci.

7. Zasady korzystania z poczty elektronicznej

1. Przesyłanie danych osobowych z użyciem poczty elektronicznej poza Spółdzielnię może odbywać się tylko przez osoby do tego upoważnione.
2. W przypadku przesyłania danych osobowych poza Spółdzielnię należy wysyłać pliki zaszyfrowane, spakowane (np. programem 7 zip, WinZip, Winrar), opatrzone hasłem, gdzie hasło powinno być przekazane odbiorcy telefonicznie lub za pomocą SMS.
3. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
4. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
5. Zabrania się otwierania załączników w mailach pochodzących od nieznanego odbiorcy (.zip, .xlsm, .pdf, .exe). Są to zwykle „wirusy", infekujące system operacyjny komputera oraz bardzo często pozostałe komputery w sieci.
6. Nie wolno otwierać odnośników (Hiperłącze) w mailach pochodzących od nieznanego adresata, gdyż mogą być odnośnikami do stron WWW zawierających w swoim kodzie wirusy. Użytkownik infekuje w ten sposób system operacyjny komputera oraz inne komputery w sieci Spółdzielni.
7. Należy zgłaszać ASI przypadki otrzymania podejrzanych e-maili.
8. Podczas wysyłania e-maili do wielu adresatów należy użyć metody „Ukryte do wiadomości – UDW". Zabronione jest rozsyłanie maili do wielu adresatów z

użyciem opcji „Do wiadomości".

9. Użytkownicy powinni okresowo kasować niepotrzebne e-maile.
10. Służbowe konta poczty elektronicznej odseparowane są od poczty prywatnej.
11. Służbowa poczta elektroniczna przeznaczona jest wyłącznie do wykonywania obowiązków służbowych.
12. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób.
13. Użytkownicy mają prawo korzystać z poczty e-mail dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.
14. Zabrania się użytkownikom służbowej poczty elektronicznej konfigurowania swoich kont pocztowych do automatycznego przekierowywania wiadomości na adres zewnętrzny.
15. Korzystanie z służbowego konta e-mail dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych.
16. Używając poczty użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.
17. Użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.
18. Użytkownik nie ma prawa wysyłać wiadomości zawierających dane osobowe pracowników, klientów, dostawców, kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.

8. Ochrona antywirusowa

1. Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym.
2. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe.
3. W przypadku stwierdzenia zainfekowania systemu lub pojawienia się komunikatów „np.; Twój system jest zainfekowany!, zainstaluj program antywirusowy", użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie ASI Spółdzielni.

9. Skrócony regulamin postępowania w przypadku naruszenia ochrony danych osobowych

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadomienia IODO Spółdzielni w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych.
2. Do sytuacji wymagających powiadomienia, należą:
    a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów
    b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych
    c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).
3. Do incydentów wymagających powiadomienia, należą:

a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności)
b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, dysków twardych, oprogramowania, pomyłki ASI Spółdzielni, użytkowników, utrata / zagubienie danych)
c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

4. Typowe przykłady incydentów wymagające reakcji:
   a. ślady na drzwiach, oknach i szafach wskazują na próbę włamania,
   b. dokumentacja jest niszczona bez użycia niszczarki,
   c. fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie,
   d. otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe,
   e. ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe,
   f. wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz budynku Spółdzielni bez upoważnienia Zarządu,
   g. udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej,
   h. telefoniczne próby wyłudzenia danych osobowych,
   i. kradzież, zagubienie komputerów przenośnych, nośników CD, DVD, dysków twardych, pamięci typu Flash z danymi osobowymi,
   j. maile zachęcające do ujawnienia identyfikatora i/lub hasła,
   k. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów,
   l. hasła do systemów zapisane i umieszczone w pobliżu komputera.

10. Obowiązek zachowania poufności i ochrony danych osobowych

1. Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do:
   a. przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Zarząd Spółdzielni zadaniach,
   b. zachowania w tajemnicy danych osobowych do których ma dostęp w związku z wykonywaniem zadań powierzonych przez Zarząd Spółdzielni,
   c. niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Zarząd Spółdzielni,
   d. zachowania w tajemnicy sposobów zabezpieczenia danych osobowych,
   e. ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem,
   f. do zachowania w tajemnicy danych osobowych i sposobu ich zabezpieczenia obowiązującego w Spółdzielni również po ustaniu zatrudnienia lub zlecenia.
2. Jeśli jest to przewidziane, osoba dopuszczona do przetwarzania odbywa szkolenie z zasad ochrony danych osobowych.
3. Osoby zapoznane z treścią niniejszym Regulaminem ODO lub przeszkolone

zobowiązane są podpisać Oświadczenie o obowiązku zachowania poufności.

4. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom, których tożsamości nie można zweryfikować lub osobom podszywającym się pod kogoś innego.
5. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych.
6. Zabrania się ujawniania na grupach dyskusyjnych, forach internetowych, blogach itp. jakichkolwiek szczegółów dotyczących funkcjonowania Spółdzielni, w tym informacji na temat sprzętu i oprogramowania, z jakiego korzysta Spółdzielnia, oraz informacji kontaktowych innych, niż ogólnodostępne w materiałach zewnętrznych.

11. Postępowanie dyscyplinarne

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy.
2. Postępowanie sprzeczne z powyższymi zobowiązaniami, może też skutkować odpowiedzialnością karną przewidzianą w ustawie o ochronie danych osobowych z dnia 10 maja 2018 (Dz. U. z 2018 poz. 1000)

ASI - Administrator Systemu Informatycznego Spółdzielni Mieszkaniowej w Sępólnie Krajeńskim

1. Niniejszy Regulamin został uchwalony przez Radę Nadzorczą Spółdzielni Mieszkaniowej w Sępólnie Krajeńskim w dniu 28.08.2019r. (uchwała nr 13/2019) i obowiązuje od dnia uchwalenia.
2. Traci moc „Regulamin Ochrony Danych Osobowych Spółdzielni Mieszkaniowej w Sępólnie Krajeńskim." uchwalony przez Radę Nadzorczą w dniu 29.08.2011r.

Sekretarz Rady Nadzorczej

SEKRETARZ
RADY NADZORCZEJ
Spółdzielni Mieszkaniowej
w Sępólnie Kr.

.....
Irena Goldiszewicz

Przewodniczący Rady Nadzorczej

PRZEWODNICZĄCY
RADY NADZORCZEJ SPÓŁDZIELNI MIESZKANIOWEJ
W SĘPÓLNIE KRAJEŃSKIM

.....
Roman Starzecki

RADCA PRAWNY

Przemysław Szukała