

REGULAMIN OCHRONY DANYCH OSOBOWYCH W SMB „JARY”

I. POSTANOWIENIA OGÓLNE

§ 1

1. Ochrona danych osobowych w SMB „Jary” ma na celu zapewnienie ochrony danych osobowych członkom SMB „Jary”, właścicielom lokali mieszkalnych i osobom posiadającym spółdzielcze własnościowe prawo do lokalu mieszkalnego (nie będącym członkami Spółdzielni), a także najemcom lokali mieszkalnych, użytkownikom i miejsc postojowych, dzierżawcom, osobom zajmującym lokale bez tytułu prawnego i pracownikom SMB „Jary”.*)
2. Regulamin niniejszy określa zasady przetwarzania danych osobowych i sposoby zabezpieczenia zbiorów danych osobowych będących w posiadaniu Spółdzielni, a także określa obowiązki administratora danych osobowych oraz prawa osób, których dane Spółdzielnia przetwarza.

§ 2

Przez użyte w treści regulaminu sformułowania należy rozumieć:

- 1) **dane osobowe** – każda informacja dotycząca osoby fizycznej, pozwalająca na określenie tożsamości tej osoby;
- 2) **zbiór danych** – każdy, posiadający strukturę zestaw danych osobowych dostępny według określonych kryteriów, w którym dane są przetwarzane, w szczególności: w kartotekach, skorowidzach, księgach, wykazach, rejestrach, systemach informatycznych itp.;
- 3) **przetwarzanie danych** - wszelkie operacje wykonywane na danych osobowych i ich zbiorach, w szczególności: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie i udostępnianie danych osobowych;
- 4) **usuwanie danych** – zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwala na ustalenie tożsamości osoby, której dane dotyczą;

- 5) **administrator danych osobowych** – administratorem danych osobowych członków SMB „Jary” i jej pracowników jest spółdzielnia mieszkaniowa, a w jej imieniu - Zarząd Spółdzielni;
- 6) **administrator bezpieczeństwa informacji** – osoba odpowiedzialna za bezpieczeństwo danych w systemie informatycznym, wyznaczona przez Zarząd SMB „Jary”;
- 7) **system informatyczny** – system przetwarzania informacji wraz ze związanymi z nim ludźmi oraz zasobami technicznymi i finansowanymi, który dostarcza i rozprawdza informacje.

§ 3

Celem zabezpieczenia zbiorów danych osobowych członków Spółdzielni i jej pracowników jest uniemożliwienie dostępu do zbioru danych osobom nieuprawnionym bądź zabierania ich przez osobę nieuprawnioną oraz ochrona danych przed ich uszkodzeniem lub zniszczeniem.

§ 4

1. SMB „Jary” jako administrator danych osobowych przetwarza dane osobowe swoich członków dla realizacji celów statutowych w zakresie:
 - 1) prowadzenia rejestru członków,
 - 2) prowadzenia rejestru lokali, dla których zostały założone księgi wieczyste z adnotacją o ustanowionych hipotekach,
 - 3) (skreślony),^{*)}
 - 4) sporządzania list niezbędnych dla obliczania opłat za użytkowanie lokali,
 - 5) gromadzenia i przetwarzania danych osobowych zawartych w indywidualnych aktach członków Spółdzielni,
 - 6) wywieszania list lokatorów na klatkach schodowych (za zgodą zainteresowanych).
2. SMB „Jary” jako administrator danych osobowych gromadzi i przetwarza dane osobowe swoich pracowników w zakresie określonym przepisami Kodeksu pracy.

§ 5

1. Dostęp do zbioru danych osobowych oraz do ich przetwarzania mogą mieć wyłącznie osoby, które uzyskały pisemne upoważnienie wydane przez Zarząd Spółdzielni. Wzór upoważnienia stanowi załącznik nr 1.
2. Administrator bezpieczeństwa informacji prowadzi ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych.
3. Ewidencja, o której mowa w ustępie 2, zawiera:
 - imię i nazwisko pracownika,
 - stanowisko,

- zakres, w jakim pracownik został dopuszczony do przetwarzania danych osobowych,
 - datę wydania upoważnienia,
 - identyfikator, w przypadku przetwarzania danych osobowych w systemie informatycznym.
4. Pracownik, który uzyskał upoważnienie do dostępu do zbioru danych osobowych i ich przetwarzania, powinien być zapoznany z przepisami dotyczącymi ochrony danych osobowych.
 5. Pracownik Spółdzielni, który uzyskał dostęp do zbioru danych osobowych i ich przetwarzania, zobowiązany jest do złożenia oświadczenia o zachowaniu ich w tajemnicy. Obowiązek ten istnieje również po ustaniu zatrudnienia przy przetwarzaniu danych osobowych.
 6. Upoważnienie, o którym mowa w ustępie 1 oraz oświadczenie pracownika o zachowaniu danych osobowych członków Spółdzielni i jej pracowników w tajemnicy, jest dołączane do akt osobowych pracownika. Wzór oświadczenia stanowi załącznik nr 2.
 7. Indywidualny zakres czynności pracownika dopuszczonego do przetwarzania danych osobowych powinien określać jego obowiązki wynikające z czynności związanych z przetwarzaniem danych osobowych oraz zakres odpowiedzialności pracownika za ochronę danych przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem.

II. OCHRONA DANYCH OSOBOWYCH PRZETWARZANYCH W SYSTEMIE INFORMATYCZNYM

§ 6

1. Przy obsłudze systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych, mogą być zatrudnieni wyłącznie pracownicy posiadający upoważnienie wydane przez Zarząd Spółdzielni.
2. Administratorem bezpieczeństwa informacji Zarząd SMB „Jary” wyznacza osobę pełniącą funkcję kierownika działu finansowo-księgowego, czyniąc ją odpowiedzialną za bezpieczeństwo danych osobowych gromadzonych i przetwarzanych w systemie informatycznym.
3. Administrator bezpieczeństwa informacji odpowiedzialny jest w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadkach wykrycia naruszeń w systemie zabezpieczeń.

§ 7

1. Pracownikowi zatrudnionemu przy przetwarzaniu danych osobowych w systemie informatycznym, administrator bezpieczeństwa informacji przydziela odrębny identyfikator i hasło.
2. Identyfikator powinien być wpisany do ewidencji pracowników zatrudnionych przy przetwarzaniu danych osobowych.
3. Ustalony identyfikator pracownika nie podlega zmianie w okresie jego zatrudnienia, a po wykreśleniu użytkownika z systemu informatycznego nie może być przydzielony innemu pracownikowi.
4. Hasło przydzielone pracownikowi zatrudnionemu przy przetwarzaniu danych osobowych pracownik powinien utrzymywać w tajemnicy, także po upływie jego ważności.
5. Bezpośredni dostęp do systemu informatycznego, zawierającego dane osobowe, może nastąpić wyłącznie po podaniu identyfikatora i hasła.
6. Identyfikator osoby, która utraciła uprawnienia dostępu do systemu informatycznego, zawierającego dane osobowe, należy natychmiast wyrejestrować z systemu i unieważnić jej hasło.

§ 8

1. Pracownik zatrudniony przy przetwarzaniu danych osobowych w systemie informatycznym obowiązany jest niezwłocznie powiadomić administratora bezpieczeństwa informacji, gdy:
 - 1) stwierdzi naruszenie zabezpieczenia systemu informatycznego,
 - 2) stan urządzeń, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakości komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych.
2. Administrator bezpieczeństwa informacji, po stwierdzeniu naruszenia systemu informatycznego, ma obowiązek:
 - 1) zabezpieczyć ślady pozwalające na określenie przyczyn naruszenia systemu informatycznego,
 - 2) przeanalizować i określić skutki naruszenia systemu informatycznego,
 - 3) określić czynności, które spowodowały naruszenie systemu informatycznego,
 - 4) dokonać niezbędnych korekt w systemie informatycznym polegających na zabezpieczeniu systemu przed ponownym jego naruszeniem,
 - 5) powiadomić Zarząd Spółdzielni o naruszeniu systemu informatycznego, jego przyczynach i skutkach oraz podjętych działaniach korygujących system.

§ 9

Administrator bezpieczeństwa informacji prowadzi rejestr pracowników – użytkowników systemu informatycznego, zawierający;

- imię i nazwisko pracownika (indywidualny identyfikator pracownika),
- stanowisko,
- zakres, w jaki pracownik został dopuszczony do przetwarzania danych osobowych w systemie informatycznym,
- datę wydania upoważnienia,
- datę utraty upoważnienia,

§ 10

System informatyczny powinien zapewniać odnotowanie:

- 1) daty wprowadzenia i modyfikacji danych osobowych,
- 2) identyfikatora użytkownika systemu wprowadzającego dane.

§ 11

System informatyczny służący do przetwarzania danych osobowych musi pozwalać na udostępnienie tych danych na piśmie w formie powszechnie zrozumiałej.

§ 12

1. Obszarami, w których przetwarzane są dane osobowe w systemie informatycznym są pomieszczenia o numerach:
 - na parterze: 101, 102, 103, 105, 106, 107, 108, 109, 110, 111, 113, 116, 117, 118, 119, 120, 121, 122.
 - na I piętrze: 201, 202, 203, 204, 205, 206, 207, 218 b.
2. Do pomieszczeń, o których mowa w ustępie 1, mogą mieć dostęp jedynie pracownicy Spółdzielni posiadający upoważnienie Zarządu SMB „Jary”.
3. Przebywanie osób nieuprawnionych oraz dostęp do danych osobowych wewnątrz obszaru określonego w zarządzaniu Spółdzielni jest możliwe jedynie w obecności osoby zatrudnionej przy przetwarzaniu tych danych i za zgodą Zarządu Spółdzielni.
4. Pomieszczenia, w których są przetwarzane dane osobowe, muszą być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych osobowych w taki sposób, aby uniemożliwić dostęp do nich osobom nieuprawnionych.
5. W pomieszczeniach, w których przebywają osoby postronne, monitory komputerów powinny być ustawione w taki sposób, aby uniemożliwić im wgląd w dane osobowe.

§ 13

Urządzenia i systemy informatyczne służące do przetwarzania danych osobowych zasilane energią elektryczną, powinny być zabezpieczone przed utratą tych danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

§ 14

Administrator bezpieczeństwa informacji obowiązany jest zabezpieczyć nośnik informacji, wydruki, kopie zapasowe, tak aby uniemożliwić dostęp do nich osobom nieuprawnionym lub przed ich uszkodzeniem lub zniszczeniem, zgodnie z przepisami. (Rozporządzenie ministra spraw wewnętrznych i administracji z dnia 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych Dz. U. nr 80 poz. 521).

§ 15

1. Kopie awaryjne nie powinny być przechowywane w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco.
2. Kopie awaryjne należy:
 - 1) okresowo sprawdzać pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu,
 - 2) bezzwłocznie usuwać po ustaniu ich użyteczności.

§ 16

1. Dane osobowe członka Spółdzielni mogą być udostępnione organom samorządowym SMB „Jary” rozpatrującym jego sprawę w postępowaniu wewnątrzspółdzielczym tylko w zakresie mogącym mieć znaczenie dla danej sprawy.
2. Zarząd SMB „Jary” jest zobowiązany do poinformowania członków organów samorządowych Spółdzielni, rozpatrujących sprawę członka w postępowaniu wewnątrzspółdzielczym, o przepisach dotyczących ochrony danych osobowych.
3. Udostępnienie danych osobowych przetwarzanych przez Spółdzielnię osobom fizycznym lub instytucjom publicznym może nastąpić jedynie na piśmie umotywowany wniosek, chyba że przepis szczególny stanowi inaczej.
4. Wniosek, o którym mowa w ustępie 3, może dotyczyć jedynie konkretnej osoby w konkretnej sytuacji i być zgodny z wzorem opublikowanym jako załącznik do Rozporządzenia ministra spraw wewnętrznych i administracji z dnia 3 czerwca 1998 r. w sprawie określenia wzorów wniosków

o udostępnienie danych osobowych, zgłoszenia zbioru danych do rejestracji oraz imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych – Dz. U. Nr 80 poz. 522 z póź. zm.

5. SMB „Jary” może odmówić udostępnienia danych osobowych swoich członków i pracowników, jeżeli spowodowałoby to istotne naruszenie dóbr osobistych osób, których dane dotyczą, lub innych osób.
6. Umieszczenie nazwiska i imienia członka Spółdzielni na liście lokatorów jest możliwe po uprzednim uzyskaniu jego zgody. ^{*)}

§ 17

1. Osoba, której dane przetwarzane są przez Spółdzielnię, ma prawo:
 - 1) do informacji o:
 - sposobie przetwarzania danych osobowych (ręczne przetwarzanie danych, metody informatyczne, w tym sieci komputerowej),
 - treści danych,
 - sposobie udostępnienia danych osobowych oraz odbiorcach lub kategorii odbiorców danych,
 - 2) żądania uzupełnienia, uaktualnienia i sprostowania danych osobowych.
2. Informacji, o których mowa w ust. 1, Zarząd SMB „Jary” jest zobowiązany udzielić w terminie 30 dni od daty otrzymania wniosku.

(-) Zarząd Spółdzielni

^{*)} zmiany wprowadzone uchwałą Zarządu nr 66/2011 z dnia 25.11.2011 r.

