U C H W A Ł A NR 67/2024

Zarządu Spółdzielni Mieszkaniowej "Bolesławianka"
w Bolesławcu z dnia 22.11.2024r.
Protokół nr 32/2024

W sprawie przyjęcia „Polityki ochrony danych osobowych''.

Na podstawie § 54 ust. 1 Statutu Spółdzielni Mieszkaniowej „Bolesławianka" w Bolesławcu uchwala się co następuje:

§1

W celu realizowania obowiązków wynikających z RODO[1] przyjmuje się „Politykę ochrony danych osobowych przetwarzanych przez Spółdzielnię Mieszkaniową Bolesławianka" (dalej jako „Polityka"), która stanowi załącznik do niniejszej uchwały.

§2

Do zapoznania się z Polityką oraz do jej stosowania obowiązani są wszyscy członkowie personelu Spółdzielni.

§3

Polityka obowiązuje od dnia 12 grudnia 2024 r. Z tym dniem tracą moc:
a) Uchwała nr 60/2018 Zarządu Spółdzielni Mieszkaniowej „Bolesławianka" z dnia 21 maja 2018 r., wprowadzająca „Zasady ochrony pomieszczeń i polityka kluczy",
b) „Polityka bezpieczeństwa",
c) „Instrukcja zarządzania systemem informatycznym".

§4

Wyznacza się na stanowisko Administratora Systemów Informatycznych (ASI) Pana Piotra Dziczkańca w celu wykonywania obowiązków przypisanych ASI w Polityce, związanych z zapewnieniem i wzmacnianiem cyberbezpieczeństwa zasobów oraz ciągłości działania Spółdzielni.

§5

Zobowiązuje się Głównego Specjalistę ds. organizacyjno – pracowniczych Panią Urszulę Minarską do niezwłocznego poinformowania wszystkich członków personelu Spółdzielni o fakcie przyjęcia Polityki, wskazania lokalizacji Polityki oraz udostępnienia niniejszej uchwały wraz z załącznikiem.

§6

Uchwała wchodzi w życie z dniem uchwalenia.

Członek Zarządu	Z-ca Prezesa Zarządu	Prezes Zarządu
mgr Magdalena Alama	d/s technicznych	mgr inż. Maciej Burniak
.....	mgr inż. Roman Jaworski	.....
	.....	

Otrzymują:

1. NOP
2. DE
3. NCM
4. GZM
5. ADM – 1
6. ADM – 2
7. ADM – 3
8. ADM – 4
9. TZ
10. a/a

1 Rozporządzenie 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.

POLITYKA OCHRONY DANYCH OSOBOWYCH SPÓŁDZIELNI MIESZKANIOWEJ „BOLESŁAWIANKA”

Nazwa dokumentu	Polityka ochrony danych osobowych Spółdzielni Mieszkaniowej „Bolesławianka”
Data ostatniej aktualizacji	12 grudnia 2024 r.
Osoba przygotowująca	Szymon Goździk – radca prawny
Zatwierdzający	Zarząd Spółdzielni Mieszkaniowej „Bolesławianka”

Spis treści

§ 1. Zakres przedmiotowy i podmiotowy Polityki 3
§ 2. Słownik pojęć 3
§ 3. Zadania osób odpowiedzialnych za ochronę danych osobowych 3
§ 4. Ogólne zasady przetwarzania danych osobowych 6
§ 5. Obszar przetwarzania danych osobowych 6
§ 6. Polityka kluczy 6
§ 7. Dopuszczenie osób do przetwarzania danych osobowych (upoważnienia) 7
§ 8. Informowanie osób fizycznych o przetwarzaniu ich danych osobowych (obowiązki informacyjne) 8
§ 9. Realizacja praw osób, których dane dotyczą 9
§ 10. Uwzględnianie ochrony danych w fazie projektowania, domyślna ochrona danych 9
§ 11. Usuwanie oraz okresy przechowywania danych osobowych 9
§ 12. Utrzymanie ciągłości działania oraz kopie zapasowe 10
§ 13. Analiza ryzyka 10
§ 14. Ocena skutków dla ochrony danych 11
§ 15. Postępowanie w sytuacji naruszenia zasad ochrony danych osobowych 11
§ 16. Udostępnianie danych osobowych 12
§ 17. Powierzenie przetwarzania danych osobowych 13
§ 18. Przekazywanie danych osobowych poza Europejski Obszar Gospodarczy 13
§ 19. Rejestrowanie przetwarzania danych osobowych 14
§ 20. Odpowiedzialność za naruszenie przepisów o ochronie danych osobowych 14
§ 21. Postanowienia końcowe 15
Załączniki: 16

§ 1. Zakres przedmiotowy i podmiotowy Polityki

1) Niniejsza Polityka określa zasady ochrony danych osobowych oraz osoby odpowiedzialne w Spółdzielni Mieszkaniowej „Bolesławianka".
2) Wszyscy współpracownicy Spółdzielni Mieszkaniowej „Bolesławianka" są zobowiązani do przestrzegania niniejszej Polityki wraz z jej załącznikami.

§ 2. Słownik pojęć

Występujące w niniejszym dokumencie pojęcia oznaczają:

1) **RODO** – Rozporządzenie 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;
2) **Spółdzielnia** – Spółdzielnia Mieszkaniowa "Bolesławianka" zarejestrowana w Sądzie Rejonowym dla Wrocławia - Fabryczna IX Wydział Gospodarczy Krajowego Rejestru Sądowego pod nr KRS: 0000125795, REGON: 000492865, NIP: 612-000-43-40;
3) **System informatyczny** – współpracujące ze sobą urządzenia i oprogramowania służące do cyfrowego przetwarzania informacji, w tym danych osobowych;
4) **IOD** – Inspektor ochrony danych Spółdzielni. W razie jego niewyznaczenia, obowiązki przypisane IOD w niniejszej Polityce przejmuje inna osoba wyznaczona przez Zarząd Spółdzielni;
5) **ASI** – Administrator Systemów Informatycznych, czyli osoba bezpośrednio odpowiedzialna za cyberbezpieczeństwo Spółdzielni;
6) **Użytkownik** – osoba uprawniona do przetwarzania danych osobowych w systemie informatycznym Spółdzielni;
7) **Dane osobowe** – informacje pozwalające bezpośrednio lub pośrednio zidentyfikować osobę fizyczną, w szczególności na podstawie takich danych jak imię i nazwisko, wizerunek, numer identyfikacyjny czy identyfikator internetowy;
8) **Dane osobowe szczególnych kategorii** – dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, dane genetyczne, dane biometryczne oraz dane dotyczące zdrowia i seksualności;
9) **Przetwarzanie danych osobowych** – czynności wykonywane na danych osobowych, takie 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;
10) **Naruszenie ochrony danych osobowych** - przypadkowe lub nieuprawnione ujawnienie, dostęp, zniszczenie, utracenie czy zmodyfikowanie danych osobowych.

§ 3. Zadania osób odpowiedzialnych za ochronę danych osobowych

1) **Zarząd Spółdzielni** odpowiada za:
   a) zapewnienie przetwarzania danych osobowych w Spółdzielni zgodnie z prawem;
   b) ograniczanie występowania zagrożeń dla ochrony danych osobowych;
   c) zapewnienie pomieszczeń dostosowanych do wymogów przetwarzanych w nich danych osobowych oraz niszczarek;
   d) podejmowanie decyzji o systemie szkoleń personelu z zakresu ochrony danych osobowych oraz cyberbezpieczeństwa;
   e) wyznaczenie Administratora Systemu Informatycznego (ASI) w formie uchwały;
   f) analizę obowiązku i wyznaczenie w razie potrzeby Inspektora ochrony danych (IOD) w formie uchwały oraz zgłoszenie jego wyznaczenia Prezesowi Ochrony Danych Osobowych;
   g) umożliwienie wykonywania zadań IOD;
   h) zwracanie się do IOD z prośbą o opinię, w przypadku wątpliwości co do stosowania przepisów prawnych z zakresu ochrony danych osobowych;
   i) utrwalanie w formie dokumentowej motywów decyzji podjętej niezgodnie z zaleceniami Inspektora ochrony danych.

2) **Przełożeni zatrudnionych** w Spółdzielni oraz **samodzielni specjaliści** odpowiadają za:
   a) nadzorowanie przetwarzania danych osobowych przez siebie oraz podwładnych;
   b) nadzorowanie zabezpieczeń powierzonych im pomieszczeń, w których przetwarzane są dane osobowe oraz ograniczanie występowania zagrożeń dla ochrony danych osobowych;
   c) zwracanie się do IOD z prośbą o opinię, w przypadku wątpliwości co do stosowania przepisów prawnych z zakresu ochrony danych osobowych;
   d) występowanie z wnioskiem o nadanie, zmianę lub cofnięcie uprawnień dostępu do pomieszczeń oraz elementów systemu informatycznego;

3) **Inspektor ochrony danych osobowych (IOD)** odpowiada za:
   a) informowanie personelu Spółdzielni o obowiązkach wynikających przepisów o ochronie danych osobowych i doradzanie w tej sprawie;
   b) monitorowanie przestrzegania przepisów o ochronie danych osobowych oraz niniejszej Polityki (w tym podejmuje działania zwiększające świadomość);
   c) udzielanie na żądanie personelu Spółdzielni zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
   d) współpracę z Prezesem Urzędu Ochrony Danych Osobowych, w tym pełnienie funkcji punktu kontaktowego dla niego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;
   e) opiniowanie projektów dokumentów dotyczących ochrony danych osobowych przekazanych przez Spółdzielnię;
   f) wykonywanie innych zadań przypisanych mu w niniejszej Polityce.

4) **Administrator Systemu Informatycznego (ASI)** administruje systemami informatycznymi oraz stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych informacji, zwłaszcza przed udostępnieniem ich osobom nieupoważnionym, utratę ich dostępności i integralności.

ASI jest zobowiązany w szczególności do:

a) zarządzania systemami i urządzeniami wchodzącymi w skład systemu informatycznego zgodnie z obowiązującymi przepisami i standardami w zakresie bezpieczeństwa informacji;
b) nadzoru nad prawidłową realizacją procesów dotyczących nadawania, modyfikowania i odbierania upoważnionym użytkownikom uprawnień do systemów i aplikacji przetwarzających dane osobowe;
c) zarządzania siecią komputerową;
d) przeprowadzania okresowych przeglądów stanu bezpieczeństwa oraz weryfikacji zabezpieczeń systemu i istniejących procedur zapewniających bezpieczeństwo danych;
e) informowania na bieżąco Prezesa Zarządu oraz IOD o istotnych wdrożeniach i zmianach w zabezpieczeniach systemu informatycznego;
f) nadzoru nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych;
g) nadzoru nad realizacją napraw, konserwacji oraz likwidacji urządzeń elektronicznych służących do przetwarzania danych osobowych,
h) wykonywania kopii zapasowych przetwarzanych informacji, ich zabezpieczenie oraz weryfikację poprawności tych procesów;
i) zapewnienie bezpieczniej wymiany danych sieci wewnętrznej i nadzór nad przesyłaniem danych osobowych za pośrednictwem urządzeń teletransmisji;
j) nadzór nad działaniem systemów awaryjnego zasilania serwerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych;
k) zgłaszanie Inspektorowi danych osobowych informacji niezbędnych do aktualizacji niniejszej Polityki w zakresie działalności ASI;
l) rekomendowanie Prezesowi Zarządu Spółdzielni działań dotyczących zakupu oprogramowania lub sprzętu, w celu realizacji lub podniesienia poziomu bezpieczeństwa systemów informatycznych, w tym bezpieczeństwa kopii zapasowych.

Szczegółowe obowiązki ASI określa w szczególności Załącznik nr 4 do niniejszej Polityki pt. „Zasady ochrony informacji przetwarzanych za pośrednictwem systemu informatycznego oraz plan ciągłości działania".

5) **Każdy członek personelu Spółdzielni** jest zobowiązany do:

a) znajomości przepisów z obszaru ochrony danych osobowych w zakresie niezbędnym do realizacji obowiązków służbowych;
b) przestrzegania zasad Polityki dotyczących jego stanowiska, w szczególności Zasad ochrony danych osobowych i innych istotnych informacji w Spółdzielni, stanowiących załącznik nr 1 do niniejszej Polityki;
c) zapewnienie poufności, dostępności i integralności przetwarzanych danych osobowych;
d) zachowania szczególnej staranności w trakcie wykonywania operacji przetwarzania danych osobowych;
e) stosowania się do zaleceń zarówno ASI jaki i IOD w zakresie ich specjalizacji;
f) niezwłocznego informowania IOD, przełożonego oraz ASI o wszelkich nieprawidłowościach dotyczących przetwarzania (w tym bezpieczeństwa) danych osobowych w Spółdzielni;

g) przetwarzania danych osobowych w sposób zapewniający ochronę przed naruszeniem ich poufności, dostępności i integralności.

§ 4. Ogólne zasady przetwarzania danych osobowych

1) Każdy współpracownik w Spółdzielni przed przystąpieniem do wykonywania zadań zapoznaje się Zasadami ochrony danych osobowych i innych istotnych informacji w Spółdzielni, stanowiącymi załącznik nr 1 do niniejszej Polityki i zobowiązuje się do ich przestrzegania wraz z zawarciem umowy ze Spółdzielnią albo poprzez podpisanie odrębnego oświadczenia w tym zakresie.
2) Zakres przetwarzanych danych osobowych nie może wykraczać poza potrzeby wynikające z celu ich przetwarzania, stąd zabronione jest gromadzenie danych nieistotnych oraz o większym stopniu szczegółowości niż jest to niezbędne do osiągnięcia celu ich przetwarzania.
3) Przetwarzane dane osobowe powinny być poprawne i aktualne.

§ 5. Obszar przetwarzania danych osobowych

1) Obszar przetwarzania danych osobowych stanowią wszystkie pomieszczenia zarządzane przez Spółdzielnię w których przetwarzane są dane osobowe, w szczególności sekretariat.
2) Przebywanie osób nieupoważnionych do przetwarzania danych osobowych wewnątrz obszaru, o którym mowa w ust. 1, jest dopuszczalne: albo pod warunkiem obecności osoby upoważnionej do przetwarzania tych danych, albo za zgodą Zarządu Spółdzielni oraz po podpisaniu przez takie osoby zobowiązania do zachowania poufności.
3) Budynki lub pomieszczenia, w których są przetwarzane dane osobowe, powinny być zamykane na czas nieobecności w nich osób upoważnionych do przetwarzania danych osobowych.
4) Część sekretariatu, w której obsługuje się petentów jest wyraźnie oddzielona od strefy, w których przechowuje się dane osobowe. Petenci nie mogą uzyskać dostępu do stref, w których przechowuje się dane osobowe, w tym do komputerów.
5) Serwery znajdują się wyłącznie w zamkniętych, dedykowanych szafach, niedostępnych dla osób trzecich, w tym petentów.
6) Pomieszczenia w których przetwarzane są dane osobowe są objęte systemem alarmowym.
7) Przetwarzanie danych osobowych poza wyznaczonym obszarem (np. na przenośnym sprzęcie komputerowym) możliwe jest po uzyskaniu ogólnej zgody Członka Zarządu lub bezpośredniego przełożonego (np. polecenie pracy zdalnej).

§ 6. Polityka kluczy

1) Spółdzielnia posiada wydzielone strefy dostępu do pomieszczeń.
2) Wejście do pomieszczeń wymaga użycia klucza lub kodu do alarmu, które posiadają jedynie upoważnieni współpracownicy Spółdzielni. Zarząd Spółdzielni wyznaczana współpracowników, którzy są upoważnieni do otwierania głównych drzwi do budynków oraz systemu alarmowego.
3) Klucze do pomieszczeń służbowych może uzyskać wyłącznie osoba, która spełniła łącznie następujące warunki:

a) jest zatrudniona lub pełni funkcję w Spółdzielni albo jest przedstawicielem podmiotu współpracującego z Spółdzielnią;
b) podpisała zobowiązanie do zachowania poufności danych osobowych i innych istotnych informacji przetwarzanych przez Spółdzielnię;
c) podpisała oświadczenie użytkownika kluczy, które stanowi **Załącznik nr 11** do niniejszej Polityki;
d) została odnotowana w rejestrze kluczy.

4) Rejestr kluczy jest prowadzony przez Głównego specjalistę ds. organizacyjnych i pracowniczych. Zawiera on przynajmniej następujące informacje: datę wydania klucza, datę zwrotu klucza, przeznaczenie klucza, imię, nazwisko, stanowisko oraz podpis współpracownika pobierającego i zwracającego klucz.
5) Duplikaty kluczy przechowywane są w sejfie Spółdzielni (klucze zapasowe). Ich wydanie może mieć miejsce tylko w uzasadnionych przypadkach oraz po wpisie do rejestru kluczy. Klucze zapasowe należy niezwłocznie zwrócić do sejfu po ich wykorzystaniu.

§ 7. Dopuszczenie osób do przetwarzania danych osobowych (upoważnienia)

1) Spółdzielnia upoważnia wszystkich współpracowników, w tym członków Rady Nadzorczej, do przetwarzania danych osobowych w zakresie i przez okres niezbędny do wykonania zadań na zajmowanym stanowisku lub zleconych zadań. W tym celu stosuje się następujące rodzaje dokumentów:
   a) **upoważnienia ogólne** do przetwarzania danych osobowych nadawane w formie dedykowanej klauzuli w umowie o pracę, umowie cywilnoprawnej lub w formie odrębnego, pisemnego oświadczenia, którego wzór zawiera **Załącznik nr 5a** do niniejszej Polityki;
   b) **upoważnienie szczególne** do przetwarzania danych osobowych nadawane w formie odrębnego, pisemnego oświadczenia, którego wzór zawiera **Załącznik nr 5b** do niniejszej Polityki, gdy przepis prawa wyraźnie to przewiduje, tj. w sytuacji, gdy:
      - wykonywanie zadań powierzonych pracownikowi wymaga dostępu do danych dotyczących zdrowia osoby ubiegającej się o pracę lub pracownika (art. 22^{1b} § 3 ustawy z 26 czerwca 1974 r. Kodeks pracy oraz art. 2b ust. 6 ustawy z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych);
      - współpracownik Spółdzielni powinien uzyskać dostęp do danych osób ubiegających się o świadczenia z Zakładowego Funduszu Świadczeń Socjalnych Spółdzielni;
      - współpracownik Spółdzielni powinien uzyskać dostęp do danych osobowych związanych z obsługą zgłoszeń sygnalistów zgodnie z przepisami ustawy z dnia 14 czerwca 2024 r. o ochronie sygnalistów;
   c) upoważnienia doraźne na wzorze przygotowanym przez IOD w zależności od bieżących potrzeb Spółdzielni i sytuacji upoważnianego.
2) Za nadawanie upoważnień o których mowa w pkt. 1 odpowiedzialny jest przełożony upoważnianego.
3) Upoważnienia są przechowywane w aktach osobowych zatrudnionego, któremu udzielono upoważnienia lub wraz z umową o współpracy z upoważnionym.
4) Bezpośredni przełożony zatrudnionego sprawuje bieżący nadzór nad tym, czy faktyczne dostępy użytkownika do danych osobowych przetwarzanych przez Spółdzielnię odpowiadają zakresowi upoważnień o których mowa w ust. 1.

5) W przypadku zakończeniu współpracy (np. rozwiązaniu umowy o pracę, umowy zlecenia, umowy o praktykę, stażu) bezpośredni przełożony niezwłocznie informuje ASI o zaprzestaniu korzystania z systemów informatycznych. ASI odbiera dostępy upoważnionemu. Za odebranie pozostałych dostępów odpowiedzialny jest bezpośredni przełożony.
6) Upoważnienie wygasa wraz z ustaniem współpracy albo po odwołaniu upoważnienia.
7) Bezpośredni przełożony upoważnianego lub Prezes Zarządu Spółdzielni odwołuje upoważnienie, gdy dostęp osoby upoważnionej do danych wskazanych w upoważnieniu przestanie być konieczny. W tym celu zawiadamia osobę upoważnioną o odwołaniu upoważnienia oraz dodaje do upoważnienia stosowną adnotację ze wskazaniem daty, z którą upoważnienie zostaje odwołane.
8) Członek Zarządu Spółdzielni, Rady Nadzorczej albo Inspektor ochrony danych mogą przeprowadzać kontrole faktycznego dostępu współpracowników Spółdzielni do zbiorów danych osobowych w Spółdzielni, w tym systemów informatycznych.

§ 8. Informowanie osób fizycznych o przetwarzaniu ich danych osobowych (obowiązki informacyjne)

1) Spółdzielnia, działając jako administrator danych osobowych, podczas pozyskiwania danych osobowych podaje osobie, której dane dotyczą, wszystkie informacje wymagane przez art. 13 RODO.
2) Jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą, Spółdzielnia działając jako administrator danych osobowych, podaje osobie, której dane dotyczą, następujące informacje wszystkie informacje wymagane przez art. 14 RODO.
   a) Informacje, o których mowa w art. 14 RODO, Spółdzielnia podaje:
      - w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca – mając na uwadze konkretne okoliczności przetwarzania danych osobowych;
      - jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą; lub
      - jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.
   b) Obowiązek o którym mowa w pkt. 2 nie jest realizowany, jeśli dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej, w szczególności tajemnicy zawodowej radców prawnych.
   c) Obowiązek o którym mowa w pkt. 2 nie jest realizowany, jeśli udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku - w takim przypadku Spółdzielnia udostępnia te informacje publicznie.
3) Obowiązki informacyjne o których mowa w pkt. 1 i 2 nie są realizowane, gdy osoba, której dane dotyczą, dysponuje już tymi informacjami.
4) Obowiązki informacyjne są realizowane w zwięzłej, przejrzystej i łatwo dostępnej formie, jasnym językiem oraz w taki sposób, aby można było udowodnić ich realizację.
5) Każdy członek personelu Spółdzielni, który bezpośrednio odpowiada za procesy przetwarzania danych, o których mowa w pkt. 1 i 2, odpowiada również za realizację obowiązków informacyjnych opisanych w niniejszym paragrafie. W razie wątpliwości konsultuje się z IOD.

6) Treść klauzuli obowiązku informacyjnego i sposób jego realizacji są zatwierdzane przez IOD.

§ 9. Realizacja praw osób, których dane dotyczą

1) Spółdzielnia udziela informacji osobom, których dane przetwarza, o ile te osoby zwróciły się z wnioskiem o realizację swoich praw o których mowa w art. 12-23 RODO. W szczególności są to: prawo dostępu do danych, ich sprostowania, usunięcia, przenoszenia, sprzeciwu wobec przetwarzania, a także prawa do ograniczenia przetwarzania danych.
2) Spółdzielnia ma prawo do odmowy uwzględnienia żądania osoby, której dane są przetwarzane, w przypadkach określonych w RODO. W takiej sytuacji Spółdzielnia informuje osobę, której dane dotyczą, o powodach niepodjęcia działań wraz ze wskazaniem podstawy prawnej i pouczeniem o możliwości wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych oraz skorzystania ze środków ochrony prawnej przed sądem.
3) Członek personelu Spółdzielni, do którego wpłynął wniosek o którym mowa w pkt 1 powyżej, niezwłocznie informuje o tym przełożonego i Inspektora ochrony danych Spółdzielni i konsultuje z nim sposób obsługi tego wniosku.
4) Szczegółowe zasady realizacji praw osób, których dane dotyczą, zostały określone Instrukcji realizacji praw osób, których dane dotyczą, która stanowi załącznik nr 3 do niniejszej Polityki.

§ 10. Uwzględnianie ochrony danych w fazie projektowania, domyślna ochrona danych

1) Każdy członek personelu Spółdzielni uwzględnia ochronę danych osobowych przy wdrażaniu nowych usług, produktów, narzędzi lub rozwiązań, a w razie potrzeby konsultuje się z IOD.
2) W przypadku, gdy wdrażane rozwiązanie lub proces będą wiązały się z przetwarzaniem danych osobowych, Spółdzielnia każdorazowo wdraża odpowiednie środki techniczne i organizacyjne (takie jak np. szyfrowanie, pseudonimizacja czy minimalizacja danych) w celu zapewnienia niezbędnych zabezpieczeń, by spełnić wymogi RODO i chronić prawa osób, których dane dotyczą.
3) Spółdzielnia wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności.

§ 11. Usuwanie oraz okresy przechowywania danych osobowych

1) Dane osobowe należy usunąć natychmiast po osiągnięciu celu ich przetwarzania, tj. wtedy, kiedy przestaną być potrzebne, w szczególności dla celów dowodowych.
2) Każdy członek personelu Spółdzielni jest odpowiedzialny za wykonywanie regularnych przeglądów danych osobowych, którymi zarządza pod kątem ich przydatności oraz ich usuwania w sytuacjach o których mowa w pkt. 1.
3) W przypadku ustania zatrudnienia lub współpracy, skrzynka pocztowa członka personelu Spółdzielni jest dezaktywowana w taki sposób, aby nie było możliwe wysyłanie z niej wiadomości e-mail za wyjątkiem komunikatów o dezaktywowaniu skrzynki e-mail lub z informacją o osobie zastępującej (w szczególności w formie autorespondera). W uzasadnionych przypadkach dostęp do zawartości dezaktywowanej skrzynki pocztowej

można nadać innemu członkowi personelu Spółdzielni, bez możliwości wysyłania wiadomości e-mail z dezaktywowanego adresu e-mail.

4) Dane osobowe gromadzone w procesie rekrutacyjnym są przechowywane do zakończenia procesu rekrutacji. W przypadku wyrażenia zgody na wykorzystywane danych osobowych dla celów przyszłych rekrutacji, dane osobowe są przechowywane przez 6 miesięcy.
5) Dane członków Spółdzielni przechowywane są przez okres 6 lat licząc od końca roku w którym ustało członkostwo.

§ 12. Utrzymanie ciągłości działania oraz kopie zapasowe

1) Każdy członek personelu Spółdzielni obowiązany jest niezwłocznie zgłosić Zarządowi Spółdzielni wszelkie zdarzenia mogące skutkować przerwaniem ciągłości działania Spółdzielni.
2) Zarząd Spółdzielni podejmuje decyzje o podjęciu działań w celu utrzymania ciągłości działania Spółdzielni, w szczególności poprzez łagodzenie skutków przerwania ciągłości działania Spółdzielni oraz działania prowadzące do jak najszybszego wznowienia działalności Spółdzielni na zwykłych zasadach.
3) Sposób, częstotliwość tworzenia, przechowywania oraz likwidacji kopii zapasowych danych osobowych przetwarzanych w systemie informatycznym określa załącznik nr 4 „Zasady ochrony informacji przetwarzanych za pośrednictwem systemu informatycznego oraz plan ciągłości działania".

§ 13. Analiza ryzyka

1) Spółdzielnia przeprowadza i dokumentuje analizę ryzyka naruszenia ochrony danych osobowych, uwzględniając charakter, zakres, kontekst i cel przetwarzania danych oraz wynikające z nich ryzyka dla praw i wolności osób. W tym celu:
   a) Spółdzielnia identyfikuje zagrożenia dla zbiorów danych osobowych i aktywów, w szczególności systemów informatycznych, w jakich są one przetwarzane, biorąc przy tym pod uwagę podatność tych zbiorów i aktywów na materializację ryzyka naruszenia ochrony danych osobowych;
   b) Spółdzielnia dokonuje szacowania prawdopodobieństwa wystąpienia zidentyfikowanych zagrożeń oraz ich skutków dla Spółdzielni, określając na tej podstawie ryzyko inherentne naruszenia ochrony danych osobowych;
   c) Spółdzielnia określa mechanizmy kontrolne mające na celu zabezpieczenie przed wystąpieniem oraz eskalacją skutków zagrożenia dla ochrony danych osobowych, a następnie ocenia skuteczność takich mechanizmów i na tej podstawie dokonuje oceny ryzyko rezydualnego naruszenia ochrony danych osobowych.
2) Analiza ryzyka powinna zawierać w szczególności:
   a) metodologię jej przeprowadzenia, w tym sposób postępowania ze stwierdzonym ryzykiem ze wskazaniem przyjętego poziomu ryzyka akceptowalnego;
   b) środki techniczne i organizacyjne stosowane w celu obniżenia ryzyka do poziomu akceptowalnego lub złagodzenia jego skutków;
   c) datę wykonania;
   d) osobę wykonującą;
   e) osobę akceptującą.
3) Dobór środków technicznych i organizacyjnych zabezpieczających przetwarzanie danych osobowych powinien być dostosowany do okoliczności i warunków przetwarzania danych

oraz prawdopodobieństwa i powagi zdarzeń, które mogą doprowadzić do naruszenia praw lub wolności osób, których dane są przetwarzane.

§ 14. Ocena skutków dla ochrony danych

1) Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Spółdzielnia przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych.
2) Ocena skutków dla ochrony danych jest wymagana w szczególności w przypadku:
   a) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;
   b) przetwarzania na dużą skalę szczególnych kategorii danych osobowych lub danych osobowych dotyczących wyroków skazujących i czynów zabronionych;
   c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.
3) Spółdzielnia przy analizie konieczności przeprowadzenia oceny skutków dla ochrony danych osobowych bierze pod uwagę Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony (M.P z 2019 r., poz. 666), chyba że został zastąpiony nowszym wykazem.
4) Ocena skutków dla ochrony danych osobowych przeprowadzana jest zgodnie z procedurą dokonywania oceny skutków dla ochrony danych osobowych, stanowiącą załącznik nr 9 do niniejszej Polityki.
5) Spółdzielnia dokumentuje przeprowadzenie skutków planowanych operacji przetwarzania dla ochrony danych osobowych.
6) Spółdzielnia przeprowadza ocenę skutków dla ochrony danych osobowych przy ścisłej współpracy pomiędzy członkami personelu Spółdzielni odpowiedzialnymi za planowaną operację przetwarzania danych, dla której powinna być przeprowadzona ocena skutków dla ochrony danych, IOD, a także ASI oraz podmiotem przetwarzającym, jeśli ich udział jest niezbędny:
   a) Przeprowadzenie oceny skutków dla ochrony danych inicjuje członek personelu Spółdzielni odpowiedzialny za planowaną operację przetwarzania danych, dla której powinna być przeprowadzona ocena skutków dla ochrony danych, oraz bierze w niej aktywny udział, konsultując się z IOD;
   b) IOD bierze udział w ocenie skutków dla ochrony danych poprzez udzielanie na żądanie personelu Spółdzielni zaleceń w tym zakresie i monitorowanie jej wykonania.
7) Jeżeli ocena skutków dla ochrony danych wykaże, że przetwarzanie powodowałoby wysokie ryzyko naruszenia praw i wolności osób, gdyby nie zastosowano środków minimalizujących to ryzyko, to przed rozpoczęciem przetwarzania Spółdzielnia konsultuje się z Prezesem Urzędu Ochrony Danych Osobowych.

§ 15. Postępowanie w sytuacji naruszenia zasad ochrony danych osobowych

1) Każdy członek personelu Spółdzielni ma obowiązek niezwłocznie zgłosić swojemu bezpośredniemu przełożonemu oraz Inspektorowi ochrony danych każde zauważone naruszenie ochrony danych osobowych. Obowiązek ten dotyczy również sytuacji podejrzenia naruszenia lub zagrożenia naruszeniem.
2) Każdy członek personelu Spółdzielni ma obowiązek niezwłocznie zgłosić Administratorowi Systemu Informatycznego każde zauważone naruszenie ochrony danych osobowych dotyczące systemu informatycznego. Obowiązek ten dotyczy również sytuacji podejrzenia naruszenia lub zagrożenia naruszeniem.
3) Każdy członek personelu Spółdzielni, który podejrzewa lub stwierdzi naruszenie ochrony danych osobowych dokonuje rozpoznania zdarzenia i podejmuje działania doraźne niezbędne do powstrzymania skutków naruszenia oraz ustalenia przyczyny i sprawcy takiego naruszenia.
4) W sytuacji zgłoszenia naruszenia lub podejrzenia ochrony danych osobowych, Inspektor ochrony:
   a) dokonuje rozpoznania zdarzenia, w tym przeprowadza ocenę czy dane zdarzenie dotyczy danych osobowych administrowanych albo powierzonych Spółdzielni do przetwarzania;
   b) powiadamia niezwłocznie o zaistniałym zdarzeniu i podjętych działaniach niezbędne osoby,
   c) bada zgłoszone naruszenia pod kątem wystąpienia przesłanek z art. 33 i 34 RODO, wyliczając Poziom Naruszenia zgodnie z metodyką zawartą w załączniku nr 8 do niniejszej Polityki. Jeśli w wyniku przeprowadzonego badania Koordynator ds. ochrony danych osobowych uzna, że zachodzą przesłanki określone w art. 33 i 34 RODO, zawiadamia o tym Prezes Zarządu Spółdzielni lub wyznaczoną osobę.
   d) nadzoruje prace zmierzające do przywrócenia stanu wolnego od naruszeń ochrony danych,
   e) odnotowuje naruszenie w Rejestrze naruszeń ochrony danych osobowych w Spółdzielni, którego wzór stanowi załącznik nr 8 do niniejszej Polityki.
5) Prezes Zarządu Spółdzielni, po konsultacji z Inspektorem ochrony danych, podejmuje decyzję w sprawie zgłoszenia organowi nadzorczemu naruszenia ochrony danych osobowych, o którym mowa w art. 33 RODO.
6) Szczegółowe zasady postępowania w sytuacji naruszenia ochrony danych osobowych w Spółdzielni określa Załącznik nr 2 – Instrukcja postępowania w sytuacji naruszenia ochrony danych.

§ 16. Udostępnianie danych osobowych

Ogólne zasady udostępniania danych osobowych

1) Spółdzielnia udostępnia dane osobowe innym podmiotom lub osobom trzecim wyłącznie wtedy, gdy istnieje ku temu podstawa prawna określona w art. 6 ust. 1 RODO, a w przypadku szczególnych kategorii danych w art. 9 ust. 2 RODO. W razie wątpliwości należy skonsultować się z Inspektorem ochrony danych a w razie jego niewyznaczenia z radcą prawnym bądź adwokatem Spółdzielni.
2) Spółdzielnia udostępnia dane osobowe innym podmiotom lub osobom trzecim wyłącznie w prawnie uzasadnianych celach oraz wyłącznie niezbędnym zakresie.

Szczególne zasady udostępniania danych osobowych

3) **Akta pracownicze** udostępnia się zatrudnionemu w sytuacjach określonych w przepisach prawa, po konsultacji z IOD. Akta są przeglądane wyłącznie pod nadzorem członka personelu Spółdzielni.
4) **Rejestr członków Spółdzielni** przeglądany jest wyłącznie w obecności pracownika Spółdzielni, po okazaniu dokumentu potwierdzającego tożsamość uprawnionego.
5) Zasady **szyfrowania danych osobowych w komunikacji elektronicznej** (w szczególności poprzez pocztę **e-mail** czy na **pendrive**) określa „Instrukcja szyfrowania danych przekazywanych drogą elektroniczną" stanowiąca załącznik nr 10 do niniejszej Polityki.

W razie jakichkolwiek wątpliwości zasięga się opinii IOD przed udostępnieniem danych osobowych, w szczególności w przypadkach o których mowa w pkt 3 i 4.

§ 17. Powierzenie przetwarzania danych osobowych

1) Zlecanie jakichkolwiek czynności związanych z przetwarzaniem danych osobowych podmiotom zewnętrznym w imieniu Spółdzielni lub zlecenie takich czynności Spółdzielni przez podmioty zewnętrzne może stanowić powierzenie przetwarzania danych osobowych[1]. W takiej sytuacji stosuje się odpowiednio postanowienia § 16 niniejszej Polityki a ponadto postanowienia niniejszego paragrafu.
2) Inspektor ochrony danych jest niezwłocznie informowany o zamiarze zawarcia i wypowiedzenia każdej umowy powierzenia przetwarzania danych osobowych.
3) Przed powierzeniem przetwarzania danych osobowych Spółdzielnia weryfikuje, czy podmiot przetwarzający zapewni wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. W tym celu pozyskuje się informacje publiczne, w tym na stronie internetowej podmiotu przetwarzającego, ocenia jego renomę na rynku a w razie braku tych informacji uzyskuje się je bezpośrednio od podmiotu przetwarzającego. Przeprowadzenie takiej oceny należy udokumentować, np. w postaci notatki czy wiadomości e-mail przechowywanej wraz z umową, do której taka ocena się odnosi.
4) Ocenę, czy dochodzi do powierzenia przetwarzania danych osobowych oraz ocenę podmiotu przetwarzającego przed zawarciem umowy dokonuje osoba przygotowująca umowę. W razie wątpliwości przeprowadzona on konsultacje z Inspektorem ochrony danych.
5) Powierzenie przetwarzania danych osobowych odbywa się na podstawie umowy pomiędzy Spółdzielnią a danym podmiotem, któremu zleca się lub który zleca czynności związane z przetwarzaniem danych osobowych.
6) Umowa, aneks lub postanowienia dotyczące powierzenia danych osobowych zawiera elementy obligatoryjne powierzenia danych osobowych wskazane w art. 28 RODO. Umowa powierzenia zatwierdzana jest przez Inspektora ochrony danych.
7) Umowy powierzenia przetwarzania danych osobowych są przechowywane wraz z umowami, których dotyczą (umowami podstawowymi).

§ 18. Przekazywanie danych osobowych poza Europejski Obszar Gospodarczy

[1] Do powierzenia przetwarzania danych osobowych dochodzi, gdy administrator danych osobowych zleca wykonywanie swoich zadań innemu podmiotowi (podmiotowi przetwarzającemu).

1) Spółdzielnia przekazuje dane osobowe poza Europejski Obszar Gospodarczy, pod warunkiem, że jest to niezbędne do osiągnięcia celu przetwarzania i że spełnione zostały warunki określone w Rozdziale V RODO.
2) Decyzję o takim udostępnieniu podejmuje osoba upoważniona do zawierania umów lub wydawania decyzji w tym zakresie po uprzedniej konsultacji z Inspektorem ochrony danych.

§ 19. Rejestrowanie przetwarzania danych osobowych

1) Spółdzielnia prowadzi **Rejestr czynności przetwarzania danych osobowych** zgodnie z art. 30 ust. 1 RODO.
   a) W Rejestrze czynności przetwarzania danych osobowych Spółdzielnia inwentaryzuje dane osobowe, monitoruje sposoby ich przetwarzania oraz przeprowadza testy uzasadnionego interesu w przypadku przetwarzania danych osobowych w oparciu o art. 6 ust. 1 lit. f RODO.
   b) Wzór Rejestru czynności przetwarzania danych osobowych stanowi załącznik nr 6 do niniejszej Polityki, który określa minimalny zakres informacji zgromadzonych w tym Rejestrze.
   c) Aktualizacji Rejestru czynności przetwarzania danych osobowych dokonuje Inspektor ochrony danych na podstawie informacji przekazywanych przez personel Spółdzielni.

2) Spółdzielnia prowadzi **Rejestr wszystkich kategorii czynności przetwarzania** danych osobowych zgodnie z art. 30 ust. 2 RODO.
   a) Rejestr obejmuje wszystkie kategorie czynności przetwarzania danych osobowych dokonywanych w imieniu innych administratorów danych osobowych.
   b) Wzór Rejestru wszystkich kategorii czynności przetwarzania stanowi załącznik nr 7 do niniejszej Polityki, który określa minimalny zakres informacji zgromadzonych w tym Rejestrze.
   c) Aktualizacji Rejestru wszystkich kategorii czynności przetwarzania dokonuje Inspektor ochrony danych na podstawie informacji przekazywanych przez personel Spółdzielni. W szczególności osoby opiniujące lub przygotowujące umowę powierzenia przetwarzania danych osobowych po stronie Spółdzielni każdorazowo przesyłają taką umowę do Inspektora ochrony danych.

3) Spółdzielnia prowadzi **Rejestr naruszeń ochrony danych osobowych** zgodnie z art. 33 ust. 5 RODO.
   a) Spółdzielnia w Rejestrze naruszeń ochrony danych osobowych dokumentuje w szczególności okoliczności naruszenia ochrony danych osobowych, jego skutki, wylicza poziom naruszenia zgodnie z przyjętą metodologią oraz podjęte działania zaradcze.
   b) Wzór rejestru naruszeń ochrony danych osobowych stanowi Załącznik nr 8 do niniejszej Polityki, który określa minimalny zakres informacji zgromadzonych w tym rejestrze.
   c) Wpisów w rejestrze dokonuje Inspektor ochrony danych.

§ 20. Odpowiedzialność za naruszenie przepisów o ochronie danych osobowych

1) Naruszenie przepisów o ochronie danych osobowych jest zagrożone sankcjami karnymi określonymi w art. 107 i 108 ustawy o ochronie danych osobowych z dnia 10 maja 2018 r. oraz w art. 266 - 269, 287 Kodeksu karnego.

2) Niezależnie od odpowiedzialności przewidzianej w przepisach, o których mowa w ust. 1, naruszenie zasad przetwarzania (w tym zabezpieczania) danych osobowych obowiązujących w Spółdzielni może zostać uznane za ciężkie naruszenie obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

§ 21. Inspektor ochrony danych

1) Inspektor ochrony danych:
   a) podlega bezpośrednio Prezesowi Zarządu Spółdzielni;
   b) nie przyjmuje poleceń lub instrukcji co do sposobu i trybu wykonywania swoich zadań;
   c) decyduje o zakresie i sposobie wykorzystania przydzielonych mu środków organizacyjnych, technicznych i finansowych do wykonywania swoich zadań;
   d) nie wykonuje zadań i obowiązków, które są jednocześnie przedmiotem jego monitorowania lub nadzoru, za wyjątkiem sytuacji, gdy możliwe jest uniknięcie konfliktu interesów, zwłaszcza gdy wykonywanie takich zadań jest poddane kontroli organu Spółdzielni;
   e) nie powinien wykonywać zadań związanych z kompetencjami i odpowiedzialnością za zarządzanie przetwarzaniem danych lub za administrowanie bezpieczeństwem przetwarzania danych;
   f) jest upoważniony do dostępu do wszelkich danych osobowych przetwarzanych przez Spółdzielnię w zakresie niezbędnym do wykonywania jego zadań,
   g) raportuje podejmowane działania w zestawieniu wykonanych czynności, udostępnianemu Prezesowi Zarządu.
2) Spółdzielnia zapewnia IOD niezwłoczną możliwość spotkań z personelem Spółdzielni w celu realizowania zadań jego zadań, udostępniając wszelkie niezbędne zasoby, w tym sprzęt elektroniczny, pomieszczenia i dokumenty.

§ 22. Postanowienia końcowe

1) Przyjęcie oraz zmiany niniejszej Polityki następują w formie uchwały Zarządu Spółdzielni.
2) Niniejszą Politykę udostępnia się w zasobach elektronicznych, dostępnych dla członków personelu w Spółdzielni.
3) Niniejsza Polityka jest poddawana przeglądowi przynajmniej raz na 2 lata i w razie potrzeby jest uaktualniana.

Załączniki:

Załącznik nr 1 – Zasady przetwarzania danych osobowych w Spółdzielni;

Załącznik nr 1 –
Zasady przetwarzania

Załącznik nr 2 – Instrukcja postępowania w sytuacji naruszenia ochrony danych;

Załącznik nr 2 -
Instrukcja postępowar

Załącznik nr 3 – Instrukcja realizacji praw osób, których dane dotyczą;

Załącznik nr 3 –
Instrukcja realizacji pr.

Załącznik nr 4 – Zasady ochrony informacji przetwarzanych w systemach informatycznych oraz plan ciągłości działania;

Załącznik nr 4 –
Zasady ochrony inforı

Załącznik nr 5a – Wzór upoważnienia do przetwarzania danych osobowych dla osób bez zawartych umów;

Wzór upoważnienia
dla osób, które zawar

Załącznik nr 5b – Wzór szczególnego upoważnienia do przetwarzania danych osobowych dotyczących zdrowia pracowników, sygnalistów oraz na potrzeby ZFŚS;

Wzór upoważnienia
dla osób, które zawar

Załącznik nr 6 – Wzór Rejestru czynności przetwarzania danych osobowych Spółdzielni;

Rejestr czynności
przetwarzania.xlsx

Załącznik nr 7 – Wzór Rejestru wszystkich kategorii czynności przetwarzania Spółdzielni;

Rejestr kategorii czynności przetwarzar

Załącznik nr 8 – Wzór Rejestru naruszeń ochrony danych osobowych Spółdzielni wraz z metodyką wyliczania poziomu naruszenia.

Rejestr naruszeń ochrony danych osob

Załącznik nr 9 – Procedura dokonywania oceny skutków dla ochrony danych osobowych

Procedura dokonywania oceny

Załącznik nr 10 – Instrukcja szyfrowania danych przesyłanych drogą elektroniczną

Instrukcja szyfrowana danych przesyłanych

Załącznik nr 11 – Powierzenie kluczy oraz kodu do alarmu

Powierzenie kluczy oraz kodu do alarmu

Załącznik nr 1 do Polityki ochrony danych osobowych

ZASADY OCHRONY DANYCH OSOBOWYCH I INNYCH ISTOTNYCH INFORMACJI W SPÓŁDZIELNI MIESZKANIOWEJ „BOLESŁAWIANKA"

Poniższe zasady obowiązują wszystkich współpracowników Spółdzielni.

1. **Zgłaszanie naruszeń ochrony danych osobowych**

   Każdy współpracownik Spółdzielni powinien niezwłocznie powiadomić Inspektora ochrony danych Spółdzielni (telefonicznie lub na iod@smbol.pl) oraz przełożonego o wszelkich zauważonych naruszeniach ochrony danych osobowych (lub podejrzeniach). Jeśli naruszenie dotyczy systemu informatycznego (e-mail, sprzęt, oprogramowanie) to należy poinformować również obsługę informatyczną Spółdzielni (ASI).

   Przykłady naruszeń: ujawnienie danych osobie nieupoważnionej, przesłanie korespondencji do niewłaściwego adresata, wyrzucenie dokumentacji bez użycia niszczarki, korzystanie z prywatnej poczty e-mail w celach służbowych, wynoszenie danych osobowych na zewnątrz bez upoważnienia, pojawienie się wirusa komputerowego, kradzież bądź zgubienie nośników z danymi osobowymi.

2. **Miejsce pracy**

   Każdy współpracownik Spółdzielni organizuje stanowisko pracy zapewniające ochronę danych osobowych i tajemnic Spółdzielni, uwzględniając wskazówki przełożonych. Należy dbać o właściwe ustawienie monitora tak, aby uniemożliwić osobom nieupoważnionym (w szczególności petentom) odczytywanie informacji z ekranu.

3. **Zasada czystego biurka**

   Na stanowisku pracy powinny znajdować się wyłącznie te dokumenty, które są aktualnie wykorzystywane i niezbędne do powierzonych zadań. Nie wolno pozostawiać dokumentów bez opieki. Wszystkie dokumenty powinny być zabezpieczone przed dostępem osób trzecich, zwłaszcza po zakończeniu pracy.

4. **Zasada czystego kosza**

   Nieprzydatne dokumenty papierowe i miękkie nośniki danych zawierające dane osobowe powinny być niszczone w sposób trwale uniemożliwiający ich odczytanie (w niszczarce).

5. **Zasada czystego ekranu**

   Przed pozostawieniem włączonego komputera bez nadzoru zatrudniony powinien się wylogować (np. używając jednocześnie klawiszy WINDOWS oraz L), jeśli mogą mieć do niego dostęp osoby nieupoważnione. Należy również pamiętać o poprawnym wyłączeniu sprzętu po zakończeniu pracy.

6. **Zasada poufności haseł i kodów dostępu**

   Każdy współpracownik Spółdzielni jest zobowiązany do zachowania poufności i nieprzekazywania innym osobom udostępnionych mu haseł i kodów dostępu. W wyjątkowych sytuacjach i za zgodną przełożonego można udostępnić innemu współpracownikowi hasło dostępu, po czym należy je zmienić przy pierwszej okazji.

7. **Zasada czystych drukarek i skanerów**

   Dokumenty powinny być zabierane z drukarek natychmiast po wydrukowaniu. Nie należy pozostawiać żadnych dokumentów na skanerach.

8. **Wynoszenie dokumentacji i sprzętu służbowego**

   Należy ograniczać do minimum korzystanie z dokumentacji papierowej, w szczególności wynoszenie jej z budynków Spółdzielni i drukowanie. Dokumenty i urządzenia służbowe wynosimy poza miejsca wykonywania pracy jedynie w niezbędnych przypadkach, za wiedzą przełożonych, po wdrożeniu

odpowiednich zabezpieczeń. W przypadku urządzeń elektronicznych należy skonsultować się z obsługą informatyczną Spółdzielni (ASI).

9. Szyfrowanie danych udostępnianych elektronicznie

Zasady szyfrowania danych osobowych udostępnianych elektronicznie (w szczególności poprzez pocztę e-mail czy na pendrive) określa „Instrukcja szyfrowania danych przekazywanych drogą elektroniczną" dostępna w katalogu /wymiana/RODO/ na dysku wspólnym.

10. Przenośne urządzenia służbowe (laptopy, telefony, inne nośniki danych)

Nie wolno pozostawiać urządzenia służbowego (zwłaszcza sprzętu komputerowego i telefonu) bez nadzoru, np. w samochodzie. Zabronione jest odstępowanie urządzeń służbowych osobom trzecim. Urządzenia służbowe muszą być zaszyfrowane podczas ich wynoszenia z budynków Spółdzielni.

W związku z korzystaniem z zasobów systemów i aplikacji służących do przetwarzania danych, każdy współpracownik mający do nich dostęp jest zobowiązany do:

- informowania przełożonych o fakcie posiadania praw dostępu do zasobów, do których nie powinien mieć dostępu lub które są zbędne,
- wykorzystywania urządzeń służbowych jedynie do czynności związanych z wykonywanymi zadaniami służbowymi,
- dbania o bezpieczeństwo danych zapisanych na użytkowanym urządzeniu, w szczególności poprzez:
  - ustawianie haseł dostępowych do aplikacji służących do przetwarzania danych osobowych, przy czym takie hasło musi się składać z przynajmniej 12 znaków;
  - natychmiastową zmianę hasła dostępowego po jego wygenerowaniu przez informatyka (ASI) a także gdy istnieje podejrzenie, że mogło ono zostać ujawnione osobie nieupoważnionej;
- zachowania szczególnej ostrożności przy odbieraniu poczty elektronicznej przychodzącej od nieznanych adresatów lub o podejrzanej treści,
- informowania obsługi informatycznej (ASI) o każdym przypadku wystąpienia usterek w pracy komputerów lub o konieczności ręcznej aktualizacji ich oprogramowania.

10. Zasada świadomej konwersacji

Przed przekazaniem osobie uprawnionej danych osobowych i innych istotnych informacji, należy uzyskać pewność co do jej tożsamości. W razie wątpliwości należy zweryfikować osobę, prosząc o podanie tych informacji o niej, które już posiadamy. W każdym przypadku nie należy przekazywać więcej informacji niż potrzeba.

11. Zasada minimalizacji danych osobowych

Pobieramy i udostępniamy tylko te dane osobowe, które są niezbędne do realizacji zadań Spółdzielni. Dane które nie będą już potrzebne są trwale i niezwłocznie usuwane.

12. Nadawanie upoważnień do przetwarzania danych osobowych

Nadanie dedykowanego upoważnienia na wzorze określonym w Polityce ochrony danych osobowych Spółdzielni jest konieczne gdy:

- wykonywanie zadań służbowych wymaga dostępu do danych dotyczących zdrowia osoby ubiegającej się o pracę lub pracownika Spółdzielni,
- współpracownik Spółdzielni ma mieć dostęp do danych innych zatrudnionych w ramach Zakładowego Funduszu Świadczeń Socjalnych,
- osoba współpracująca ze Spółdzielnią nie zawarła umowy.

13. Lokalizacja dokumentów dotyczących ochrony danych osobowych

Polityka ochrony danych osobowych wraz z załącznikami (w tym instrukcją szyfrowania danych przesyłanych elektronicznie, instrukcją postępowania z naruszeniami ochrony danych osobowych oraz wzorami upoważnień do przetwarzania danych osobowych) jest dostępna w katalogu /wymiana/RODO/ na dysku wspólnym.

Załącznik nr 2 do Polityki ochrony danych osobowych

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH

1) „Naruszenie ochrony danych osobowych" oznacza przypadkowe lub nieuprawnione ujawnienie, dostęp, zniszczenie, utracenie czy zmodyfikowanie danych osobowych.
2) Za naruszenie lub podejrzenie naruszenia ochrony danych osobowych uznaje się w szczególności:
   a) ujawnienie danych osobowych osobie nieupoważnionej,
   b) zgubienie nośnika zawierającego dane osobowe,
   c) znalezienie niezniszczonych nośników zawierających dane osobowe w koszu na śmieci lub innym miejscu nie przeznaczonym do ich przechowywania,
   d) pozostawienie bez nadzoru osoby nieupoważnionej w pomieszczeniu, w którym przetwarza się dane osobowe,
   e) niewłaściwe działanie fizycznych zabezpieczeń pomieszczenia, w którym przetwarza się dane osobowe.
3) **Każdy współpracownik Spółdzielni ma obowiązek niezwłocznie zgłosić przełożonemu i Inspektorowi ochrony danych (IOD) każde zauważone naruszenie ochrony danych osobowych.** Obowiązek ten dotyczy również sytuacji podejrzenia naruszenia lub zagrożenia naruszeniem.
4) **Każdy współpracownik Spółdzielni ma obowiązek niezwłocznie zgłosić Administratorowi Systemu Informatycznego (ASI) każde zauważone naruszenie ochrony danych osobowych dotyczące systemu informatycznego.** Obowiązek ten dotyczy również sytuacji podejrzenia naruszenia lub zagrożenia naruszeniem.
5) Każdy współpracownik Spółdzielni, który podejrzewa lub stwierdzi naruszenie ochrony danych osobowych dokonuje rozpoznania zdarzenia i podejmuje działania doraźne niezbędne do minimalizacji skutków naruszenia oraz ustalenia przyczyny i sprawcy takiego naruszenia.
6) W sytuacji zgłoszenia naruszenia lub podejrzenia ochrony danych osobowych, Inspektor ochrony danych:
   a) dokonuje rozpoznania zdarzenia, w tym przeprowadza ocenę czy dane zdarzenie dotyczy danych osobowych administrowanych albo powierzonych Spółdzielni do przetwarzania;
   b) powiadamia niezwłocznie o zaistniałym zdarzeniu i podjętych działaniach niezbędne osoby,
   c) bada zgłoszone naruszenia pod kątem wystąpienia przesłanek z art. 33 i 34 RODO, wyliczając Poziom Naruszenia zgodnie z metodyką zawartą w załączniku nr 8 do niniejszej Polityki. Jeśli w wyniku przeprowadzonego badania Inspektor ochrony danych osobowych uzna, że zachodzą przesłanki określone w art. 33 i 34 RODO, zawiadamia o tym Prezesa Zarządu Spółdzielni lub wyznaczoną osobę.
   d) nadzoruje prace zmierzające do przywrócenia stanu wolnego od naruszeń ochrony danych,
   e) odnotowuje naruszenie w Rejestrze naruszeń ochrony danych osobowych, którego wzór stanowi załącznik nr 8 do niniejszej Polityki.
7) Prezes Zarządu Spółdzielni, po konsultacji z Inspektorem ochrony danych, podejmuje decyzję w sprawie zgłoszenia organowi nadzorczemu naruszenia ochrony danych osobowych, o którym mowa w art. 33 RODO. W przypadku podjęcia decyzji o zgłoszeniu

naruszenia organowi nadzorczemu, Spółdzielnia dokonuje takiego zgłoszenia bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia.

8) Spółdzielnia bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o naruszeniu ochrony danych osobowych w Spółdzielni, powodującym wysokie ryzyko naruszenia praw lub wolności takiej osoby, chyba że wystąpi jedna z poniższych przesłanek:
   a) zaistniałe naruszenie nie powoduje wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
   b) Spółdzielnia wdrożyła odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności: szyfrowanie uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
   c) Spółdzielnia zastosowała środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą.
9) Zawiadomienia dokonuje się w formie mailowej lub pisemnej. Jeśli zawiadomienie wymagałoby niewspółmiernie dużego wysiłku, Spółdzielnia może:
   a) wydać publiczny komunikat, m.in. na swojej stronie internetowej, zawierający wymaganą treść;
   b) zastosować inny środek, za pomocą którego osoby, których dane dotyczą, zostaną poinformowane w równie skuteczny sposób o naruszeniu, zawierający wymaganą treść.
10) Zawiadomienie powinno czynić zadość wymaganiom określonym w art. 34 ust. 2 RODO tj. powinno opisywać możliwe konsekwencje naruszenia ochrony danych osobowych, opisywać środki zastosowane lub proponowane przez Spółdzielnię w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Załącznik nr 3 – Instrukcja realizacji praw osób, których dane dotyczą

INSTRUKCJA REALIZACJI PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ

§1. Cel

Celem niniejszej instrukcji jest zapewnienie zasad i procedury realizacji praw osób, których dane osobowe przetwarza Spółdzielnia Mieszkaniowa „Bolesławianka" w Bolesławcu jako administrator danych osobowych (dalej „osoby, których dane dotyczą") w rozumieniu 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 (dalej „RODO").

§2. Osoby odpowiedzialne

Każdy współpracownik Spółdzielni, który przetwarza dane osobowe, odpowiedzialny jest za realizację praw osób, których dane dotyczą w zakresie swojego stanowiska.

§3. Zakres Instrukcji

Niniejsza instrukcja określa zasady i procedury realizacji następujących praw osób, których dane dotyczą określonych w Rozdziale III RODO:

1) udzielenie informacji – spełnienie obowiązku informacyjnego;
2) zapewnienie dostępu do danych osobowych;
3) sprostowanie i uzupełnienie danych osobowych;
4) usunięcie danych osobowych (prawo do bycia zapomnianym);
5) ograniczenie przetwarzania danych osobowych;
6) sprzeciw;
7) przenoszenie danych;
8) prawo do tego, by nie podlegać profilowaniu.

§4. Zasady ogólne w zakresie realizacji praw

1) Żądanie osoby, której dane dotyczą, może zostać zgłoszone w dowolnej formie.
2) Ilekroć osoba, której dane dotyczą, zgłosi żądanie realizacji danego prawa, w przypadku zaistnienia uzasadnionych wątpliwości w zakresie tożsamości tej osoby, współpracownik Spółdzielni żąda dodatkowych informacji (które już posiada) od osoby, której dane dotyczą, w celu potwierdzenia jej tożsamości.
3) Personel Spółdzielni udziela odpowiedzi na każde zgłoszone żądanie realizacji prawa bez zbędnej zwłoki, jednakże nie później niż w terminie 1 miesiąca od dnia otrzymania danego żądania, z zastrzeżeniem ust. 7 poniżej. Odpowiedzi udziela się w tej samej formie, w której żądanie zostało zgłoszone, chyba, że osoba, której dane dotyczą, zażąda udzielenia odpowiedzi w innej formie.
4) W wyjątkowych sytuacjach tj. z uwagi na skomplikowany charakter żądania lub liczbę żądań w danym okresie, personel Spółdzielni jest uprawniony do przedłużenia terminu realizacji żądania o kolejne 2 miesiące. W takim przypadku informuje on o tym osobę, której dane

dotyczą, nie później niż w terminie 1 miesiąca od dnia otrzymania żądania, uzasadniając swoją decyzję oraz informując o możliwości wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych oraz skorzystania ze środków ochrony prawnej przed sądem.

5) W przypadku, gdy żądanie jest oczywiście nieuzasadnione lub nadmierne, Spółdzielnia może odmówić działań lub pobrać za nie określoną opłatę. Spółdzielnia dokumentuje fakt, że żądanie ma oczywiście nieuzasadniony lub nadmierny charakter. W takim wypadku Spółdzielnia informuje o tym osobę, której dane dotyczą, niezwłocznie, jednakże nie później niż w terminie 1 miesiąca od dnia otrzymania żądania, uzasadniając swoją decyzję oraz informując o możliwości wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych oraz skorzystania ze środków ochrony prawnej przed sądem.
6) W przypadku, gdy nie ma podstaw do realizacji do żądania osoby, której dane dotyczą, współpracownik Spółdzielni informuje o tym osobę, której dane dotyczą, w terminie, o którym mowa w ust. 4 powyżej, wskazując powody niepodejmowania działań oraz informując o możliwości wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych oraz skorzystania ze środków ochrony prawnej przed sądem.
7) Spółdzielnia informuje o sprostowaniu, uzupełnieniu, usunięciu lub ograniczeniu przetwarzania danych osobowych każdego odbiorcę, któremu ujawniono dane osobowe wnioskodawcy, chyba, że byłoby to niemożliwe lub wymagające niewspółmiernie dużego wysiłku. W przypadku zaistnienia któregokolwiek z tych wyjątków, współpracownik Spółdzielni sporządza notatkę ze stosownym uzasadnieniem.

§5. Zapewnienie dostępu do danych osobowych

1) Każda osoba fizyczna ma prawo zgłoszenia żądania uzyskania informacji, czy Spółdzielnia przetwarza jej dane osobowe, a jeśli tak, ma prawo żądania uzyskania dostępu do tych danych oraz informacji, o których mowa art. 15 RODO, tj.:
   a) cele przetwarzania;
   b) kategorie odnośnych danych osobowych;
   c) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
   d) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
   e) informacje o prawie do żądania sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
   f) informacje o prawie wniesienia skargi do organu nadzorczego;
   g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;
   h) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania.
2) Spółdzielnia, na żądanie osoby, której dane dotyczą, dostarcza jej również kopię danych osobowych podlegających przetwarzaniu.
3) Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o

odpowiednich zabezpieczeniach, o których mowa w art. 46 RODO, związanych z przekazaniem.

§6. Sprostowanie i uzupełnienie danych

1) Każda osoba, której dane dotyczą, ma prawo żądania sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych.
2) Spółdzielnia dokonuje sprostowania lub uzupełnienia w sposób odpowiadający okolicznościom danego procesu przetwarzania, np. poprzez przedstawienie osobie, której dane dotyczą, dodatkowego formularza do wypełnienia; prośbę o przesłanie drogą tradycyjną lub elektroniczną prawidłowych/uzupełnionych danych.
3) Spółdzielnia informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, których dokonał zgodnie z art. 16 RODO (prawo do sprostowania danych), art. 17 ust. 1 RODO (prawo do usunięcia danych) i art. 18 RODO (prawo do ograniczenia przetwarzania), każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Spółdzielnia informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

§7. Usunięcie danych („prawo do bycia zapomnianym")

1) Każda osoba, której dane dotyczą, ma prawo żądania od Spółdzielnia usunięcia dotyczących jej danych osobowych, jeżeli zachodzi jedna z następujących okoliczności:
   a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
   b) osoba, której dane dotyczą, cofnęła zgodę będąca podstawą do przetwarzania danych zgodnie z art. 6 ust. 1 lit. a) RODO, a brak jest innej podstawy przetwarzania;
   c) osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania danych, o którym mowa w § 9 poniżej i nie występują okoliczności, o których mowa w § 10 ust. 2 poniżej;
   d) dane osobowe są przetwarzane niezgodnie z prawem;
   e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii Europejskiej lub prawie polskim;
   f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.
2) W celu realizacji prawa, o którym mowa w ust. 1 powyżej, współpracownik Spółdzielni obsługujący żądanie zapewnia poinformowanie i wydanie stosownych instrukcji wszystkim współpracownikom Spółdzielni, którzy przetwarzają dane określonej osoby, we współpracy z Administratorem Systemu Informatycznego.

§8. Ograniczenie przetwarzania danych

1) Każda osoba, której dane dotyczą ma prawo żądania od Spółdzielni ograniczenia przetwarzania jej danych osobowych, w przypadku gdy:
   a) kwestionuje ona prawidłowość danych osobowych – na okres pozwalający Spółdzielni sprawdzić prawidłowość tych danych;
   b) przetwarzanie jest niezgodne z prawem, a osoba sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;

c) Spółdzielnia nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie do ustalenia, dochodzenia lub obrony roszczeń;
d) osoba, której dane dotyczą wniosła sprzeciw wobec przetwarzania danych, o którym mowa w § 9 poniżej – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie Spółdzielni są nadrzędne wobec podstaw sprzeciwu.

2) W przypadku wykonania żądania realizacji prawa, o którym mowa w ust. 1 powyżej, Spółdzielnia dokonuje oznaczenia danych objętych żądaniem i zaprzestaje ich przetwarzania w inny sposób niż ich przechowywanie, chyba że:
a) osoba, której dane dotyczą, wyrazi zgodę na inny sposób przetwarzania danych,
b) jest to niezbędne w celu ustalenia, dochodzenia lub obrony roszczeń,
c) jest niezbędne w celu ochrony praw innej osoby fizycznej lub prawnej,
d) z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego.

3) W przypadku uchylenia ograniczenia przetwarzania danych osobowych, Spółdzielnia informuje o tym osobę, której dane dotyczą.

§9. Sprzeciw

1) Każda osoba, której dane dotyczą, ma prawo wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – w przypadku, gdy Spółdzielnia przetwarza dane na następujących podstawach:
a) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Spółdzielni;
b) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Spółdzielnie 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;
c) w tym profilowania na podstawie przepisów art. 6 ust. 1 lit. e i f RODO wymienionych powyżej w punktach a) oraz b).

2) Ust. 1 powyżej nie dotyczy sytuacji, gdy istnieją ważne, prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby, której dane dotyczą lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

3) Każda osoba, której dane dotyczą, ma prawo wnieść sprzeciw w przypadku, gdy jej dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim.

4) W celu realizacji prawa, o którym mowa w ust. 1 powyżej, współpracownik Spółdzielni rozpatrujący sprzeciw zapewnia poinformowanie i wydanie stosownych instrukcji pozostałym współpracownikom Spółdzielni, którzy przetwarzają w swoich jednostkach organizacyjnych dane określonej osoby, we współpracy z Administratorem Systemu Informatycznego.

§10. Przenoszenie danych

1) Każda osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, dane osobowe jej dotyczące,

które dostarczyła Spółdzielni, oraz ma prawo żądać przesłania tych danych osobowych innemu administratorowi danych osobowych, jeżeli:

a) przetwarzanie odbywa się na podstawie zgody lub na podstawie niezbędności do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie tej osoby przed zawarciem umowy, oraz
b) przetwarzanie odbywa się w sposób zautomatyzowany.

2) Jeżeli jest to technicznie możliwe, na żądanie osoby, której dane dotyczą, Spółdzielnia przesyła dane bezpośrednio innemu administratorowi danych osobowych.
3) Współpracownik Spółdzielni rozpatrujący żądanie, we współpracy z Administratorem Systemu Informatycznego, z uwagi na różnorodność procesów przetwarzania danych w Spółdzielni, każdorazowo podejmują decyzję co do sposobu realizacji prawa do przenoszenia danych, przedstawiając ją do akceptacji Członka Zarządu Spółdzielni.

Załącznik nr 4 do Polityki ochrony danych osobowych

ZASADY OCHRONY INFORMACJI PRZETWARZANYCH W SYSTEMACH INFORMATYCZNYCH

Niniejszy dokument ma na celu zapewnienie najwyższego poziomu poufności i dostępności danych osobowych oraz innych istotnych informacji przy wykonywaniu obowiązków Spółdzielni wynikających z art. 24 ust. 1, art. 25 ust. 1, art. 32 ust. 1 lit b i d oraz art. 32 ust. 2 RODO. W szczególności celem niniejszego dokumentu jest zapobieganie naruszeniom poufności w postaci nieuprawnionego dostępu do danych osobowych i innych istotnych informacji oraz zapewnienie ciągłości działania, w tym utrzymanie zdolności do szybkiego przywrócenia tych danych.

I. Dostęp do zasobów informatycznych

1) Uwierzytelnienie użytkownika w systemach informatycznych Spółdzielni następuje przynajmniej za pomocą unikalnego loginu i hasła. Dopuszcza się stosowanie wyjątków od tej zasady w uzasadnionych okolicznościach, w szczególności dla kont testowych.
2) Działania użytkowników w systemach informatycznych są rejestrowane.
3) Prawa dostępu poszczególnych użytkowników do wskazanego zakresu danych w ramach systemu informatycznego (w tym zbiorów danych osobowych), nadaje się w jedynie w zakresie niezbędnych do wykonywania powierzonych im obowiązków. Realizacja tego obowiązku spoczywa w szczególności na Administratorze Systemów Informatycznych (ASI) oraz na bezpośrednich przełożonych użytkowników.
4) ASI stosuje automatyczną blokadę dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności użytkownika. Blokada aktywuje się po 5 minutach.
5) Zapewnia się ciągłe monitorowanie ruchu sieciowego w celu rejestrowania i przeciwdziałania nieautoryzowanym działaniom w systemie informatycznych, w tym wyciekom danych.
6) W przypadku zdalnego dostępu użytkowników do informacji umieszczonych w zasobach Spółdzielni stosuje się połączenia szyfrowanie.
7) Stosuje się szyfrowanie nośników danych, które mają być użytkowane poza siedzibą Spółdzielni, zwłaszcza laptopów i dysków zewnętrznych.

II. Nadawanie i zmiana uprawnień użytkowników

1) Dostęp do systemu informatycznego może uzyskać wyłącznie osoba, która spełniła łącznie następujące warunki:
   a) jest zatrudniona w Spółdzielni lub na innej podstawie współpracuje ze Spółdzielnią (np. jest przedstawicielem podmiotu współpracującego ze Spółdzielnią albo pełni swoją funkcję pro bono);
   b) podpisała zobowiązanie do zachowania poufności danych osobowych i innych istotnych informacji przetwarzanych w Spółdzielni;
   c) została zarejestrowana jako użytkownik w systemie informatycznym Spółdzielni.
2) Do konta użytkownika przypisane są również uprawnienia dostępowe do poszczególnych programów komputerowych, a także do poszczególnych plików lub folderów. Zakres tych uprawnień określa ASI lub przełożony użytkownika.
3) Rejestracji użytkownika dokonuje ASI na wniosek skierowany do niego drogą mailową przez przełożonego użytkownika. Wniosek zawiera informacje, o których mowa w pkt 2. ASI informuje przełożonego o rejestracji użytkownika.

III. Odebranie uprawnień użytkowników

1) ASI odbiera uprawnienia użytkownikowi na wysłany e-mailem wniosek bezpośredniego przełożonego. Odebranie uprawnień może mieć charakter czasowy lub trwały. ASI informuje bezpośredniego przełożonego użytkownika o odebraniu uprawnień.
2) Przełożony składa wniosek o odebranie uprawnień użytkownikowi, niezwłocznie gdy:
   a) użytkownik zakończy współpracę ze Spółdzielnią,
   b) Spółdzielnia poweźmie informacje o celowym naruszeniu przez użytkownika zobowiązania do zachowania poufności,
   c) nastąpi długotrwała przerwa w świadczeniu usług lub pracy przez użytkownika na rzecz Spółdzielni,
   d) zostało wszczęte wobec użytkownika będącego pracownikiem postępowanie dyscyplinarne,
   e) zostało wszczęte postępowanie sądowe wobec podmiotu współpracującego ze Spółdzielnią, którego użytkownik jest przedstawicielem.

IV. Hasła użytkowników

1) ASI w przypadku dodawania nowego użytkownika w systemie informatycznym generuje nazwę konta oraz pierwsze hasło i przekazuje je użytkownikowi.
2) Użytkownik systemu po otrzymaniu pierwszego hasła w momencie rozpoczęcia pracy w systemie jest zobowiązany do zmiany otrzymanego hasła, jeśli to możliwe.
3) Hasło wpisywane przez użytkownika nie jest wyświetlane. Po trzecim z kolei podaniu nieprawidłowego hasła, konto użytkownika zostaje zablokowane w systemie informatycznym.
4) Użytkownik zobowiązuje się do zachowania hasła w poufności. W szczególności zabronione jest utrwalanie haseł w sposób jawny.
5) Hasła, w stosunku do których zaistniało podejrzenie nieuprawnionego ujawnienia, podlegają bezzwłocznej zmianie.
6) W wyjątkowych sytuacjach, takich jak nieobecność użytkownika, hasło może zostać udostępnione jego zastępcy za zgodą bezpośrednio przełożonego albo ASI. Po ustaniu sytuacji awaryjnej użytkownik jest zobowiązany do niezwłocznej zmiany hasła.
7) Hasło powinno się składać:
   a) z przynajmniej 12 znaków;
   b) jednej małej i dużej litery;
   c) jednej cyfry;
   d) jednego znaku specjalnego.
8) Hasło nie może:
   a) zawierać popularnych, powszechnie używanych słów czy wyrażeń;
   b) zawierać elementów nazwy Spółdzielni lub identyfikatora użytkownika;
   c) zawierać słów w języku angielskim.
9) ASI blokuje możliwość ustawienia hasła znajdującego się na liście słabych/często używanych haseł opracowywanego przez CERT Polska[1] lub inne zaufane źródło.
10) ASI stosuje bezpieczny algorytm hashujący do przechowywania haseł[2].

[1] https://cert.pl/uploads/2022/01/hasla/resources/wordlist_pl.zip
[2] Szczegóły: https://cert.pl/posts/2022/01/rekomendacje-techniczne-systemow-uwierzytelniania/

11) ASI deponuje w zabezpieczonej kopercie w sejfie Prezesa Zarządu Spółdzielni hasła do kluczowych elementów systemu informatycznego Spółdzielni. Ten obowiązek podlega bezpośredniemu nadzorowi przez Prezesa Zarządu Spółdzielni.
12) W przypadku utraty uprawnień przez ASI należy niezwłocznie zmienić jego hasło. Ten obowiązek podlega bezpośredniemu nadzorowi Prezesa Zarządu Spółdzielni.
13) Wymogi określone w pkt. 1-12 nie mają zastosowania do systemów, w zakresie w jakim procedury dotyczące haseł do tych systemów zostały uregulowane odrębnymi regulacjami wewnętrznymi w Spółdzielni.

VI. Korzystanie z systemu informatycznego Spółdzielni przez użytkowników

1) Użytkownik jest zobowiązany do uniemożliwienia osobom nieupoważnionym (w szczególności petentom Spółdzielni oraz kurierom) wglądu do informacji wyświetlanych na monitorze jego komputera.
2) Przed dłuższym opuszczeniem stanowiska służbowego, użytkownik zobowiązany jest zablokować ekran albo wylogować się.
3) Po zakończeniu pracy, użytkownik zobowiązany jest:
   a) wylogować się z systemu informatycznego, a następnie wyłączyć urządzenie;
   b) zabezpieczyć stanowisko pracy, w szczególności zabezpieczyć wszelką dokumentację oraz nośniki, na których znajdują się dane osobowe oraz inne istotne informacje.
4) Użytkownik szyfruje dane przesyłane elektronicznie, w szczególności przekazywane za pośrednictwem poczty elektronicznej, zgodnie z „Instrukcją szyfrowania danych przekazywanych drogą elektroniczną", która jest dostępna w katalogu /wymiana/RODO/ na dysku wspólnym. Użytkownik konsultuje się z ASI w razie potrzeby.
5) Nieuzasadnione z punktu widzenia wykonywania obowiązków służbowych kopiowanie plików z danymi osobowymi jest zabronione.
6) Użytkownicy nie są uprawnieni do przesyłania informacji uzyskanych przy wykonywaniu obowiązków służbowych, za pośrednictwem komunikatorów czy mediów społecznościowych, za wyjątkiem aplikacji dostarczonych albo zweryfikowanych i zaakceptowanych przez Spółdzielnię, po rekomendacji ASI.
7) Użytkownicy tworząc pliki w systemie informatycznym nazywają je w sposób przejrzysty i czytelny.

VII. Korzystanie z sieci publicznej

1) Sieć wewnętrzna Spółdzielni jest odseparowana od sieci publicznej.
2) Zabrania się użytkownikom wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim lub innym naruszającym prawo a także pornograficznym.

VIII. Korzystanie z poczty elektronicznej

1) Poczta e-mail Spółdzielni może być wykorzystywana jedynie do celów służbowych, w szczególności zabronione jest przechowywanie prywatnych wiadomości na służbowej skrzynce e-mail.
2) Użytkownicy nie są uprawnieni do korzystania z prywatnej skrzynki poczty elektronicznej oraz prywatnych kont w serwisach internetowych w celach służbowych.

IX. Dostępność danych osobowych i innych istotnych informacji oraz kopie zapasowe

1) Spółdzielnia podejmuje niezbędne działania, a ASI rekomenduje rozwiązania, aby w razie wystąpienia incydentu, system informatyczny i wdrożone zabezpieczenia organizacyjne i techniczne, zapewniały zdolność do szybkiego przywrócenia dostępu do przetwarzanych w tym systemie danych osobowych.
2) ASI wykonuje kopie zapasowe, które w przypadku awarii są wykorzystywane do odtworzenia systemu operacyjnego, aplikacji i innych danych systemu informatycznego służącego do przetwarzania danych osobowych.
3) ASI sprawuje nadzór nad wykonywaniem kopii zapasowych oraz weryfikuje poprawność tego procesu a także likwiduje niepotrzebne kopie zapasowe.
4) W celu zapewnienia poprawności wykonywanych kopii zapasowych ASI przeprowadza regularne testy ich integralności.

X. Zewnętrzne nośniki danych

1) Zewnętrzne nośniki danych będące w zasobach Spółdzielni (np. pendrive) zawierające dane osobowe i inne istotne informacje są oznaczane i przechowywane w odpowiednich, bezpiecznych, zamykanych szafach lub sejfach, znajdujących się w siedzibie Spółdzielni.
2) Wynoszenie nośników zewnętrznych zawierających dane osobowe poza siedzibę Spółdzielni jest dopuszczalne wyłącznie uzasadnionych przypadkach, za zgodą przełożonego.
3) Nośniki i urządzenia zawierające dane osobowe wynoszone poza siedzibę Spółdzielni zabezpiecza się w sposób zapewniający poufność i integralność danych, w szczególności poprzez ich szyfrowanie. Sposób zabezpieczenia określa się w porozumieniu z ASI.
4) Użytkownik szyfruje dane udostępniane elektronicznie, w szczególności przekazywane na pendrive, zgodnie z „Instrukcją szyfrowania danych przekazywanych drogą elektroniczną" dostępna w katalogu /wymiana/RODO/ na dysku wspólnym. Użytkownik konsultuje się z ASI w razie potrzeby.
5) Likwidacja uszkodzonych lub niepotrzebnych nośników zawierających dane osobowe odbywa się przez fizyczne zniszczenie nośnika w sposób uniemożliwiający odczytanie zawartych na nim danych albo poprzez jego pełne formatowanie. Szybkie formatowanie jest zabronione.

XI. Zasady postępowania ze służbowymi urządzeniami przenośnymi (komputery przenośne, tablety, telefony komórkowe)

1) Przetwarzanie danych osobowych przy użyciu służbowych urządzeń przenośnych może odbywać się za zgodą ASI i Członka Zarządu.
2) Jeżeli specyfika służbowego urządzenia przenośnego na to pozwala, ASI stosuje środki ochrony kryptograficznej lub bardziej zaawansowane zabezpieczenia. Wszystkie urządzenia przenośne zawierające dane osobowe, wynoszone poza siedzibę Spółdzielni są szyfrowane, chyba że Prezes Zarządu Spółdzielni postanowi inaczej.
3) Użytkownik służbowego urządzenia przenośnego zabezpiecza hasłem dostęp do tego urządzenia, jeżeli jest to możliwe. W razie wątpliwości użytkownik konsultuje zabezpieczenie urządzenia z ASI.

4) Użytkownik służbowego urządzenia przenośnego zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych.
5) Użytkownik służbowego urządzenia przenośnego w szczególności nie powinien udostępniać tego urządzenia osobom nieupoważnionym do przetwarzania dostępnych na nim danych osobowych oraz nie powinien pozostawiać tego urządzania bez nadzoru w miejscach publicznych.
6) W razie zgubienia lub kradzieży służbowego urządzenia przenośnego użytkownik zobowiązany jest do natychmiastowego powiadomienia ASI, IOD oraz przełożonego.

XII. Ochrona antywirusowa

1) W celu ochrony systemu informatycznego przed skutkami szkodliwego działania oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, zakłada się możliwość stosowania następujących zabezpieczeń:
   - wyłączenie nieużywanych usług systemu operacyjnego,
   - regularną aktualizację oprogramowania, w tym baz wirusów,
   - uaktywnienie logów systemowych o ile jest to możliwe;
   - stosowanie szyfrowanych kanałów dostępu z sieci zewnętrznych do sieci wewnętrznej (VPN, szyfrowanie plików i poczty),
   - stosowanie szyfrowania danych na serwerach,
   - stosowanie firewall,
   - filtracja połączeń sieciowych za pomocą serwera Proxy,
   - zamknięcie niewykorzystywanych portów służących do transmisji danych;
   - stosowanie oprogramowania antywirusowego i antyspamowego na serwerach, stacjach roboczych użytkowników w sieci wewnętrznej i urządzeniach przenośnych,
   - ochrona styku sieci wewnętrznej Spółdzielni z sieciami zewnętrznymi,
   - sieć bezprzewodową zabezpiecza się technologią WPA2 lub silniejszymi zabezpieczeniami.
2) W celu minimalizowania możliwości przedostania się szkodliwego oprogramowania do systemu informatycznego stosuje się następujące rozwiązania:
   a) zabrania się użytkownikom instalacji bez zgody ASI jakiegokolwiek oprogramowania;
   b) zabrania się użytkownikom dokonywania jakichkolwiek zmian w konfiguracji zainstalowanego oprogramowania, w szczególności oprogramowania antywirusowego.
3) ASI odpowiada za prawidłowe działania ochrony antywirusowej, w tym za zapewnienie odpowiedniej liczby licencji oprogramowania antywirusowego dla stacji roboczych użytkowników.
4) W przypadku stwierdzenia podejrzanego zachowania wskazującego na wirusa, użytkownik winien niezwłocznie powiadomić przełożonego, ASI oraz IOD.

XIII. Przeglądy i konserwacja systemu informatycznego w tym dostęp podmiotów zewnętrznych

1) ASI odpowiada za sprawną pracę systemu informatycznego, w tym w szczególności stacji roboczych, aplikacji serwerowych, baz danych, poczty email.
2) ASI zapewnia bieżące aktualizacje oprogramowania zgodnie z zaleceniami producentów.

3) Przegląd i konserwacja systemu informatycznego powinny być wykonywane w terminach określonych przez producentów systemu lub zgodnie z harmonogramem ASI.
4) ASI rekomenduje niezbędne optymalizacje zasobów serwerowych i stacji roboczych.
5) ASI zapewnia, że zakupione na podstawie jego rekomendacji oprogramowania jest licencjonowane.
6) Wszelkie prace konserwacyjne i naprawcze sprzętu komputerowego oraz uaktualnienia systemu informatycznego są wykonywane z uwzględnieniem zasad ochrony danych osobowych i cyberbezpieczeństwa.
7) Miejsca i ich otoczenie, w których znajdują się systemy informatyczne Spółdzielni powinny być monitorowane podczas przeprowadzanych tam prac, w szczególności prac wykonywanych przez podmioty zewnętrzne w celu uniknięcia zniszczenia danych, ich kradzieży oraz uniemożliwienia instalacji tam oprogramowania mogącego wpływać na bezpieczeństwo danych.

XIV. Analiza ryzyka przetwarzania informacji za pośrednictwem systemu informatycznego

1) Spółdzielnia dokonuje doboru skutecznych środków technicznych i organizacyjnych adekwatnie do poziomu ustalonych ryzyk, na podstawie rekomendacji ASI.
2) ASI we współpracy z IOD przeprowadza udokumentowaną analizę ryzyka dla procesów przetwarzania informacji za pośrednictwem systemu informatycznego zgodnie z § 13. Polityki ochrony danych osobowych.
3) ASI rekomenduje dobór środków bezpieczeństwa w oparciu o stan wiedzy technicznej, który powinno się oceniać z uwzględnieniem warunków rynkowych, w szczególności dostępności i akceptowalności rynkowej danego rozwiązania technicznego.
4) Analiza ryzyka jest akutalizowana raz do roku oraz w razie:
   - zmiany dostawcy narzędzia służącego do przetwarzania danych osobowych,
   - wprowadzania nowych funkcjonalności czy istotnych ulepszeń do systemu informatycznego,
   - pełnego restartu systemu informatycznego.
5) Wyniki analizy ryzyka są udostępniane IOD oraz Prezesowi Zarządu Spółdzielni.

XV. Regularne testowanie, mierzenie i ocenianie skuteczności środków ochrony informacji przetwarzanych za pośrednictwem systemu informatycznego

1) ASI odpowiada za bieżące i regularne testowanie, mierzenie i ocenianie skuteczności środków ochrony informacji przetwarzanych za pośrednictwem systemu informatycznego Spółdzielni.
2) Przeprowadzoną ocenę zabezpieczeń i przeprowadzone testy należy dokumentować. Zauważone błędy i podatności powinny być regularnie usuwane, a jeśli jest to niemożliwe wdrażane są inne środki zaradcze.

PLAN CIĄGŁOŚCI DZIAŁANIA
(dalej jako „Plan")

PODMIOT PLANU:
Spółdzielnia Mieszkaniowa "Bolesławianka" zarejestrowana w Sądzie Rejonowym dla Wrocławia - Fabryczna IX Wydział Gospodarczy Krajowego Rejestru Sądowego pod nr KRS: 0000125795, REGON: 000492865, NIP: 612-000-43-40

RODZAJ DZIAŁALNOŚCI:
Zarządzanie zasobem mieszkaniowym Spółdzielni oraz zaspokajanie potrzeb mieszkaniowych i innych potrzeb członków oraz ich rodzin.

SKŁAD ZESPOŁU ODPOWIEDZIALNEGO ZA REALIZACJĘ PLANU
1. Prezes Zarządu Spółdzielni (Szef zespołu kryzysowego);
2. Administrator Systemu Informatycznego Spółdzielni;
3. Inspektor ochrony danych Spółdzielni, jeśli został powołany.

CEL PLANU
Spółdzielnia dąży do zapewnienia ciągłości działania w przypadku nagłej, niespodziewanej i nieprzewidywalnej przeszkody uniemożliwiającej bieżące prowadzenie działalności. Celem Planu jest określenie zasad postępowania prowadzących do wznowienia działalności w możliwie najkrótszym czasie od momentu zaistnienia przestoju w prowadzonej działalności.

Do zdarzeń, które mogą spowodować przestój w świadczeniu usług zalicza się m.in.
- Pożar;
- Powódź;
- Zawalenie budynku;
- Utrata znaczącej części personelu;
- Odcięcie dostępu do energii elektrycznej;
- Awaria systemu komputerowego, w tym atak hackerski;
- Awaria sytemu telefonicznego;
- Pandemia.

TRYB POSTĘPOWANIA ZESPOŁU KRYZYSOWEGO
1. Prezes Zarządu, a w razie jego nieobecności Zastępca (Szef zespołu kryzysowego), podejmuje decyzję o wdrożeniu Planu wraz z scenariuszem adekwatnym do zaistniałego zdarzenia powodującego istotne ryzyko przestoju w świadczeniu usług, po konsultacji z ASI.
2. Osoba wyznaczona przez Szefa zespołu kryzysowego informuje mieszkańców oraz klientów Spółdzielni o istotnej, czasowej utracie możliwości wykonywania zadań, nie później niż w ciągu 24 godz. od otrzymania informacji o sytuacji awaryjnej.
3. Osoba wyznaczona przez Szefa zespołu kryzysowego informuje mieszkańców oraz klientów Spółdzielni o ustaniu sytuacji awaryjnej nie później niż w ciągu 24 godz. od otrzymania informacji o jej ustaniu.
4. Zabrania się komunikowania z mediami przez członków personelu Kancelarii z wyłączeniem osób wyznaczonych przez Szefa zespołu kryzysowego.

SCENARIUSZE KRYZYSOWE

W zależności od możliwego scenariusza zdarzeń w niniejszym Planie zostały określone następujące strategie ciągłości działania, skutkujące ograniczeniem działalności Spółdzielni i występowaniem problemów z realizowaniem swoich zadań:

Lp.	Scenariusz	Ryzyko	Tryb pracy	Osoba/jednostka odpowiedzialna za wdrożenie działania
1.	**Budynki** Brak dostępu do siedziby Spółdzielni lub jej części na skutek np. pożaru, zalania, naruszenia konstrukcji	Istotność wpływu (1-3): 3 Prawdopodobieństwo (1-3): 1 Ryzyko (1-9): **3**	Polecenie wszystkim lub części pracownikom pracy zdalnej. W razie potrzeby Administrator Systemów Informatycznych dokonuje przywrócenia danych z kopii zapasowej na serwerze w lokalizacji zapasowej.	Prezes Zarządu
2.	**Zasoby IT** Utrata infrastruktury IT, uszkodzenie lub zniszczenie urządzeń lub elementów technologicznych	Istotność wpływu (1-3): 1-3 w zależności od liczby i roli urządzeń Prawdopodobieństwo (1-3): 2 Ryzyko (1-9): **2-6**	Praca na urządzeniach zapasowych i działania na rzecz przywrócenia podstawowych (pierwotnych) zasobów IT. W razie potrzeby Administrator Systemów Informatycznych dokonuje przywrócenia danych z kopii zapasowej na serwerze w lokalizacji zapasowej.	Administrator Systemu Informatycznego (ASI)
3.	**Zasoby ludzkie** Utrata kluczowych pracowników, np. masowe odejścia z pracy, strajki, sabotaż	Istotność wpływu (1-3): 3 Prawdopodobieństwo (1-3): 1 Ryzyko (1-9): **3**	Doraźnie: propozycja pracy w godzinach nadliczbowych dla pozostałego personelu Docelowo: uzupełnienie braków kadrowych poprzez rekrutacje, ewentualnie współpracę z podmiotami wspomagającymi proces rekrutacji.	Prezes Zarządu, przełożony dotknięty skutkami scenariusza
4.	**Pandemia** Izolacja pracowników w domach, brak możliwości wykonywania pracy w budynkach Spółdzielni	Istotność wpływu (1-3): 1 Prawdopodobieństwo (1-3): 2 Ryzyko (1-9): **2**	Polecenie wszystkim lub części pracownikom pracy zdalnej, wdrożenie wytycznych organów policji gospodarczej (np. Głównego Inspektora Sanitarnego, Państwowej Inspekcji Pracy).	Prezes Zarządu
5.	**Cyberatak** Użycie szkodliwego oprogramowania lub nieautoryzowany dostęp do danych w celu ich kradzieży, modyfikacji lub zniszczenia	Istotność wpływu (1-3): 3 Prawdopodobieństwo (1-3): 2 Ryzyko (1-9): **6**	Odcięcie zagrożonych elementów systemu Spółdzielni, praca na urządzeniach zapasowych i działania na rzecz przywrócenia pierwotnych zasobów IT. W razie potrzeby Administrator Systemów Informatycznych dokonuje przywrócenia danych z kopii zapasowej na serwerze w lokalizacji zapasowej.	Administrator Systemu Informatycznego (ASI)
6.	**Awaria zasilania** Brak dostępności kluczowej infrastruktury IT, zakłócenia w komunikacji teleinformatycznej	Istotność wpływu (1-3): 3 Prawdopodobieństwo (1-3): 1 Ryzyko (1-9): **3**	W zależności od rozmiarów awarii zasilenia, tj. zasięgu i czasu trwania: 1) Praca na urządzeniach zapasowych, w tym zapasowych źródłach zasilania, 2) Przekazanie zadań innym pracownikom, którzy nie zostali dotknięci awarią zasilania, 3) Przemieszczenie pracowników do miejsc pracy zdalnej zapewniających bezpieczeństwo przetwarzania danych, gdzie dostępne jest zasilanie i sieć teleinformatyczna, zaakceptowanych przez Spółdzielnię.	Administrator Systemu Informatycznego (ASI)

Metodologia wyliczenia ryzyka dla danego scenariusza kryzysowego:

a) Ryzyko w skali od 1 do 9 oblicza się mnożąc „Istotność wpływu" oraz „Prawdopodobieństwo".

b) Istotność wpływu określa się w skali 1 do 3, gdzie im wyższa wartość, tym większa istotność negatywnego wpływu danego scenariusza na ciągłość działania.
c) Prawdopodobieństwo określa się w skali 1 do 3, gdzie im wyższa wartość, tym większe prawdopodobieństwo wystąpienia danego scenariusza na ciągłość działania.

Zmiana miejsca pracy

W przypadku czynnika zagrożenia będącego przeszkodą uniemożliwiającą bieżące świadczenie usług podejmuje się następujące czynności:

a) Pracownikom poleca się pracę zdalną w zakresie w jakim jest to możliwe.

b) Wszystkie niezbędne środki trwałe są niezwłocznie dostarczane personelowi Spółdzielni do miejsc świadczenia pracy wraz z niezbędnym sprzętem informatycznym i biurowym.

c) W razie przerwy w świadczeniu usług, w pierwszej kolejności następuje poinformowanie członków Spółdzielni o zaistniałej sytuacji oraz o potrzebie zastosowania Planu. Za zapewnienie przekazania tych informacji odpowiedzialny jest Szef zespołu kryzysowego.

d) W przypadku utraty serwerów z powodu nagłego, niespodziewanego i nieprzewidywalnego zdarzenia w pierwszej kolejności uruchamia się usługi świadczone członkom Spółdzielni w sposób ciągły, w szczególności za pośrednictwem internetu.

e) Administrator Systemu Informatycznego dysponuje i zarządza kopiami zapasowymi zgodnie z postanowieniami „ZASAD OCHRONY INFORMACJI PRZETWARZANYCH W SYSTEMACH INFORMATYCZNYCH", stanowiących załącznik nr 4 do Polityki ochrony danych osobowych przetwarzanych w Spółdzielni.

f) Administrator Systemu Informatycznego dokonuje odtworzenia konfiguracji systemów z kopii zapasowych w następującej kolejności:
   - Przywrócenia bazy danych;
   - Uprawnienia, udostępnienia, przydziały dyskowe;
   - Przywrócenie poczty;
   - Test.

Przypadki o charakterze przejściowych przeszkód z pozostaniem w dotychczasowym miejscu świadczenia usług

a) W przypadku wystąpienia sytuacji, w której osoba nieupoważniona ingeruje w sposób niedozwolony w sieć informatyczną Spółdzielni, próbuje modyfikować informacje lub wprowadza złośliwe kody, Administrator Systemu Informatycznego dokonuje fizycznego odcięcia systemu oraz jego zabezpieczenia.

b) W przypadku zniszczenia sieci informatycznej Spółdzielni w wyniku wystąpienia nagłego, niespodziewanego i nieprzewidywalnego zdarzenia, Administrator Systemu Informatycznego dokonuje odtworzenia konfiguracji systemów z kopii zapasowych na serwerze w następującej kolejności:
   - Przywrócenia bazy danych;
   - Uprawnienia, udostępnienia, przydziały dyskowe;
   - Przywrócenie poczty;
   - Test.

c) W sytuacji, w której w wyniku nagłego, niespodziewanego i nieprzewidywalnego zdarzenia, następuje zniszczenie zasobów użytkowników, na które składają się następujące elementy:
   - Profile,
   - Folder dokumentów użytkownika,
   - Katalog domowy,

   Administrator Systemu Informatycznego dokonuje przywrócenia danych z kopii zapasowej.

d) W przypadku uszkodzenia komputera użytkownika końcowego Administrator Systemu Informatycznego przekazuje użytkownikowi komputer zastępczy. Jednocześnie za pomocą kopii zapasowej przywraca ustawienia systemu.

PLAN ODBUDOWY

W przypadku kiedy istnienie przeszkody uniemożliwiającej wykonywanie zadań Spółdzielni związanej ze zniszczeniem jej budynków Szef zespołu kryzysowego jest odpowiedzialny za zakup i dostarczenie niezbędnego sprzętu informatycznego oraz za odbudowę zniszczonej siedziby albo znalezienie nowej.

LISTA TELEFONÓW AWARYJNYCH

1. Numer awaryjny: 112
2. Pogotowie Ratunkowe: 999
3. Policja: 997
4. Straż Pożarna: 998
5. Straż Miejska: 986
6. Stały dyżur Centrum Zarządzania Kryzysowego: (071) 371 - 67 - 04
7. Pogotowie ciepłownicze: 993
8. Pogotowie energetyczne: 991 lub 071 329 10 81
9. Pogotowie gazowe: 992
10. Pogotowie wodno-kanalizacyjne: 994 lub 071 372 40 02; 348 53 14
11. Pogotowie dźwigowe: 071 344 10 22, 351 39 66

Bolesławiec, ...r.
(data nadania upoważnienia)

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Działając w imieniu Spółdzielni Mieszkaniowej „Bolesławianka" w Bolesławcu, w celu wypełnienia obowiązków wynikających z przepisów prawa,

upoważniam Panią/Pana .....

stanowisko/funkcja .....

- do przetwarzania danych osobowych w zakresie zadań wynikających z zajmowanego stanowiska albo pełnionej funkcji. Szczegółowe informacje co do zakresu upoważnienia będą przekazywane przez przełożonych lub wynikają z przepisów prawa oraz regulacji wewnętrznych Spółdzielni, w szczególności ze Statutu.

- do przetwarzania następujących kategorii danych osobowych (należy zaznaczyć niezbędne):

  ☐ dotyczących **stanu zdrowia pracowników**[1]

  ☐ danych **pracowników niepełnosprawnych** przetwarzanych dla celów określonych w ustawie z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych

  ☐ danych **osób ubiegających się o świadczenia z Zakładowego Funduszu Świadczeń Socjalnych** Spółdzielni

  ☐ związanych z obsługą **zgłoszeń sygnalistów** w myśl przepisów ustawy z dnia 14 czerwca 2024 r. o ochronie sygnalistów

w zakresie niezbędnym do wykonywania powierzonych zadań.

Niniejsze upoważnienie przestaje obowiązywać z chwilą rozwiązania stosunku pracy bądź innego stosunku łączącego osobę upoważnioną ze Spółdzielnią Mieszkaniową „Bolesławianka" a także w przypadku odwołania ze stanowiska.

Wystawił: .....
(przełożony osoby upoważnianej)

Osoba upoważniona do przetwarzania wyżej wymienionych danych osobowych jest zobowiązana do zachowania ich w tajemnicy a także sposobów ich zabezpieczania. Obowiązek ten jest nieograniczony w czasie.
Osoba upoważniona oświadcza, że zapoznała się z zasadami ochrony danych osobowych obowiązującymi u Pracodawcy, stanowiącymi załącznik do niniejszego upoważnienia oraz zobowiązuje się do ich przestrzegania.

Przyjął: .....
(data i podpis osoby upoważnionej)

[1] Zwłaszcza informacje do celów ubezpieczeń społecznych (np. ciąża czy choroba).

Adnotacja o odwołaniu upoważnienia[2]

Z dniem ..... odwołuje się niniejsze upoważnienie w zakresie przetwarzania następujących kategorii danych osobowych (należy zaznaczyć):

- ☐ dotyczących **stanu zdrowia pracowników**
- ☐ danych **pracowników niepełnosprawnych** przetwarzanych dla celów określonych w ustawie z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych
- ☐ danych **osób ubiegających się o świadczenia z Zakładowego Funduszu Świadczeń Socjalnych** Spółdzielni
- ☐ związanych z obsługą **zgłoszeń sygnalistów** w myśl przepisów ustawy z dnia 14 czerwca 2024 r. o ochronie sygnalistów

Oświadczam, że poinformowano osobę upoważnioną o odwołaniu upoważnienia oraz odebrano mu wszystkie związane z tym dostępy (w szczególności w systemie informatycznym).

.....
(data i podpis przełożonego osoby upoważnionej)

[2] Należy wypełnić jedynie w razie odwołania upoważnienia w całości lub w części. W przypadku ustania zatrudnienia upoważnienie wygasa na mocy postanowień Polityki ochrony danych osobowych, stąd nie jest konieczne wypełnianie „Adnotacji o odwołaniu upoważnienia" w takiej sytuacji.

ZASADY OCHRONY DANYCH OSOBOWYCH I INNYCH ISTOTNYCH INFORMACJI W SPÓŁDZIELNI MIESZKANIOWEJ „BOLESŁAWIANKA"

Poniższe zasady obowiązują wszystkich współpracowników Spółdzielni.

1. Zgłaszanie naruszeń ochrony danych osobowych

Każdy współpracownik Spółdzielni powinien niezwłocznie powiadomić Inspektora ochrony danych Spółdzielni (telefonicznie lub na iod@smbol.pl) oraz przełożonego o wszelkich zauważonych naruszeniach ochrony danych osobowych (lub podejrzeniach). Jeśli naruszenie dotyczy systemu informatycznego (e-mail, sprzęt, oprogramowanie) to należy poinformować również obsługę informatyczną Spółdzielni (ASI).
Przykłady naruszeń: ujawnienie danych osobie nieupoważnionej, przesłanie korespondencji do niewłaściwego adresata, wyrzucenie dokumentacji bez użycia niszczarki, korzystanie z prywatnej poczty e-mail w celach służbowych, wynoszenie danych osobowych na zewnątrz bez upoważnienia, pojawienie się wirusa komputerowego, kradzież bądź zgubienie nośników z danymi osobowymi.

2. Miejsce pracy

Każdy współpracownik Spółdzielni organizuje stanowisko pracy zapewniające ochronę danych osobowych i tajemnic Spółdzielni, uwzględniając wskazówki przełożonych. Należy dbać o właściwe ustawienie monitora tak, aby uniemożliwić osobom nieupoważnionym (w szczególności petentom) odczytywanie informacji z ekranu.

3. Zasada czystego biurka

Na stanowisku pracy powinny znajdować się wyłącznie te dokumenty, które są aktualnie wykorzystywane i niezbędne do powierzonych zadań. Nie wolno pozostawiać dokumentów bez opieki. Wszystkie dokumenty powinny być zabezpieczone przed dostępem osób trzecich, zwłaszcza po zakończeniu pracy.

4. Zasada czystego kosza

Nieprzydatne dokumenty papierowe i miękkie nośniki danych zawierające dane osobowe powinny być niszczone w sposób trwale uniemożliwiający ich odczytanie (w niszczarce).

5. Zasada czystego ekranu

Przed pozostawieniem włączonego komputera bez nadzoru zatrudniony powinien się wylogować (np. używając jednocześnie klawiszy WINDOWS oraz L), jeśli mogą mieć do niego dostęp osoby nieupoważnione. Należy również pamiętać o poprawnym wyłączeniu sprzętu po zakończeniu pracy.

6. Zasada poufności haseł i kodów dostępu

Każdy współpracownik Spółdzielni jest zobowiązany do zachowania poufności i nieprzekazywania innym osobom udostępnionych mu haseł i kodów dostępu. W wyjątkowych sytuacjach i za zgodną przełożonego można udostępnić innemu współpracownikowi hasło dostępu, po czym należy je zmienić przy pierwszej okazji.

7. Zasada czystych drukarek i skanerów

Dokumenty powinny być zabierane z drukarek natychmiast po wydrukowaniu. Nie należy pozostawiać żadnych dokumentów na skanerach.

8. Wynoszenie dokumentacji i sprzętu służbowego

Należy ograniczać do minimum korzystanie z dokumentacji papierowej, w szczególności wynoszenie jej z budynków Spółdzielni i drukowanie. Dokumenty i urządzenia służbowe wynosimy poza miejsca wykonywania pracy jedynie w niezbędnych przypadkach, za wiedzą przełożonych, po wdrożeniu odpowiednich zabezpieczeń. W przypadku urządzeń elektronicznych należy skonsultować się z obsługą informatyczną Spółdzielni (ASI).

9. Szyfrowanie danych udostępnianych elektronicznie

Zasady szyfrowania danych osobowych udostępnianych elektronicznie (w szczególności poprzez pocztę e-mail czy na pendrive) określa „Instrukcja szyfrowania danych przekazywanych drogą elektroniczną" dostępna w katalogu /wymiana/RODO/ na dysku wspólnym.

10. Przenośne urządzenia służbowe (laptopy, telefony, inne nośniki danych)

Nie wolno pozostawiać urządzenia służbowego (zwłaszcza sprzętu komputerowego i telefonu) bez nadzoru, np. w samochodzie. Zabronione jest odstępowanie urządzeń służbowych osobom trzecim. Urządzenia służbowe muszą być zaszyfrowane podczas ich wynoszenia z budynków Spółdzielni.
W związku z korzystaniem z zasobów systemów i aplikacji służących do przetwarzania danych, każdy współpracownik mający do nich dostęp jest zobowiązany do:

- informowania przełożonych o fakcie posiadania praw dostępu do zasobów, do których nie powinien mieć dostępu lub które są zbędne,
- wykorzystywania urządzeń służbowych jedynie do czynności związanych z wykonywanymi zadaniami służbowymi,
- dbania o bezpieczeństwo danych zapisanych na użytkowanym urządzeniu, w szczególności poprzez:
  - ustawianie haseł dostępowych do aplikacji służących do przetwarzania danych osobowych, przy czym takie hasło musi się składać z przynajmniej 12 znaków;
  - natychmiastową zmianę hasła dostępowego po jego wygenerowaniu przez informatyka (ASI) a także gdy istnieje podejrzenie, że mogło ono zostać ujawnione osobie nieupoważnionej;
- zachowania szczególnej ostrożności przy odbieraniu poczty elektronicznej przychodzącej od nieznanych adresatów lub o podejrzanej treści,
- informowania obsługi informatycznej (ASI) o każdym przypadku wystąpienia usterek w pracy komputerów lub o konieczności ręcznej aktualizacji ich oprogramowania.

11. Zasada świadomej konwersacji

Przed przekazaniem osobie uprawnionej danych osobowych i innych istotnych informacji, należy uzyskać pewność co do jej tożsamości. W razie wątpliwości należy zweryfikować osobę, prosząc o podanie tych informacji o niej, które już posiadamy. W każdym przypadku nie należy przekazywać więcej informacji, niż potrzeba.

12. Zasada minimalizacji danych osobowych

Pobieramy i udostępniamy tylko te dane osobowe, które są niezbędne do realizacji zadań Spółdzielni. Dane które nie będą już potrzebne są trwale i niezwłocznie usuwane.

13. Nadawanie upoważnień do przetwarzania danych osobowych

Nadanie dedykowanego upoważnienia na wzorze określonym w Polityce ochrony danych osobowych Spółdzielni jest konieczne gdy:

a) wykonywanie zadań służbowych wymaga dostępu do danych dotyczących zdrowia osoby ubiegającej się o pracę lub pracownika Spółdzielni,
b) współpracownik Spółdzielni ma mieć dostęp do danych innych zatrudnionych w ramach Zakładowego Funduszu Świadczeń Socjalnych,
c) osoba współpracująca ze Spółdzielnią nie zawarła umowy.

14. Lokalizacja dokumentów dotyczących ochrony danych osobowych

Polityka ochrony danych osobowych wraz z załącznikami (w tym instrukcją szyfrowania danych przesyłanych elektronicznie, instrukcją postępowania z naruszeniami ochrony danych osobowych oraz wzorami upoważnień do przetwarzania danych osobowych) jest dostępna w katalogu /wymiana/RODO/ na dysku wspólnym.

Bolesławiec, ...r.
(data nadania upoważnienia)

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH DOTYCZĄCYCH ZDROWIA PRACOWNIKÓW, SYGNALISTÓW ORAZ NA POTRZEBY ZAKŁADOWEGO FUNDUSZU ŚWIADCZEŃ SOCJALNYCH

Działając w imieniu Spółdzielni Mieszkaniowej „Bolesławianka" w Bolesławcu, w celu wypełnienia obowiązków wynikających z przepisów prawa,

upoważniam Panią/Pana .....

stanowisko/funkcja .....

– do przetwarzania następujących kategorii danych osobowych (należy zaznaczyć niezbędne):

☐ dotyczących **stanu zdrowia pracowników**[1]

☐ danych **pracowników niepełnosprawnych** przetwarzanych dla celów określonych w ustawie z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych

☐ danych **osób ubiegających się o świadczenia z Zakładowego Funduszu Świadczeń Socjalnych** Spółdzielni

☐ związanych z obsługą **zgłoszeń sygnalistów** w myśl przepisów ustawy z dnia 14 czerwca 2024 r. o ochronie sygnalistów

w zakresie niezbędnym do wykonywania powierzonych zadań.

Niniejsze upoważnienie przestaje obowiązywać z chwilą rozwiązania stosunku pracy bądź innego stosunku łączącego osobę upoważnioną ze Spółdzielnią Mieszkaniową „Bolesławianka" a także w przypadku odwołania ze stanowiska.

Wystawił: .....
(przełożony osoby upoważnianej)

Osoba upoważniona do przetwarzania wyżej wymienionych danych osobowych jest zobowiązana do zachowania ich w tajemnicy a także sposobów ich zabezpieczania. Obowiązek ten jest nieograniczony w czasie.

Przyjął: .....
(data i podpis osoby upoważnionej)

[1] Zwłaszcza informacje do celów ubezpieczeń społecznych (np. ciąża czy choroba).

Adnotacja o odwołaniu upoważnienia[2]

Z dniem ..... odwołuje się niniejsze upoważnienie w zakresie przetwarzania następujących kategorii danych osobowych (należy zaznaczyć):

☐ dotyczących **stanu zdrowia pracowników**

☐ danych **pracowników niepełnosprawnych** przetwarzanych dla celów określonych w ustawie z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych

☐ danych **osób ubiegających się o świadczenia z Zakładowego Funduszu Świadczeń Socjalnych** Spółdzielni

☐ związanych z obsługą **zgłoszeń sygnalistów** w myśl przepisów ustawy z dnia 14 czerwca 2024 r. o ochronie sygnalistów

Oświadczam, że poinformowano osobę upoważnioną o odwołaniu upoważnienia oraz odebrano mu wszystkie związane z tym dostępy (w szczególności w systemie informatycznym).

.....
(data i podpis przełożonego osoby upoważnionej)

[2] Należy wypełnić jedynie w razie odwołania upoważnienia w całości lub w części. W przypadku ustania zatrudnienia upoważnienie wygasa na mocy postanowień Polityki ochrony danych osobowych, stąd nie jest konieczne wypełnianie „Adnotacji o odwołaniu upoważnienia" w takiej sytuacji.