POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH W SPÓŁDZIELNI MIESZKANIOWEJ „NA KOZŁÓWCE”

Kraków, 25.04.2025]

wersja 2.0

	Imię i Nazwisko	Stanowisko służbowe	Data	Podpis
Opracował				
Sprawdził				
Zatwierdził:		Rada Nadzorcza		

1 SPIS TREŚCI

2 INFORMACJE OGÓLNE

Polityka Bezpieczeństwa Danych Osobowych określa zasady przetwarzania danych osobowych w **Spółdzielni Mieszkaniowej „Na Kozłówce"** w Krakowie, w celu zapewnienia ich bezpieczeństwa. Bezpieczeństwo danych jest rozumiane jako zapewnienie:

- poufności – dane nie są dostępne dla osób nieupoważnionych;
- dostępności – dane są dostępne i użyteczne na żądanie osób upoważnionych;
- integralności danych i systemów, w których dane są przetwarzane – dane nie są zmienione lub zniszczone w sposób nieautoryzowany.

Niniejszą **Politykę** stosuje się do wszystkich danych osobowych przetwarzanych w Spółdzielni, niezależnie od formy, zakresu przetwarzania oraz lokalizacji zbioru.

W przedstawionej dokumentacji za Administratora Danych (AD) rozumie się **Spółdzielnię Mieszkaniową „Na Kozłówce" z siedzibą w Krakowie, ul. Spółdzielców 3, 30-682 Kraków.**

Ochrona danych osobowych przetwarzanych w **Spółdzielni Mieszkaniowej „Na Kozłówce"** (zwana dalej Administratorem, AD lub Spółdzielnią) obowiązuje wszystkie osoby (bez względu na zajmowane stanowisko oraz miejsce wykonywania, jak również charakter stosunku pracy), które mają dostęp do danych osobowych zbieranych, przetwarzanych oraz przechowywanych w Spółdzielni w związku z prowadzoną działalnością. Na potrzeby niniejszej **Polityki**, za pracownika uznaje się wszystkie te osoby (w tym stażystów, praktykantów oraz osoby zatrudnione na umowę zlecenie lub o dzieło). Osoby mające dostęp do danych osobowych zobowiązane są do stosowania środków określonych w niniejszej **Polityce**, regulacjach wewnętrznych Spółdzielni oraz innych aktach prawnych, z którymi pracownik został zapoznany. Środki te mogą wiązać pracownika zarówno podczas trwania stosunku pracy jak i po jego ustaniu.

3 PODSTAWA PRAWNA

Podstawą do opracowania niniejszego dokumentu i jego wdrożenia są następujące przepisy prawa:

a) Konstytucja Rzeczypospolitej Polskiej;
b) Rozporządzenie 2016/679 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.
c) Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych;
d) Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania 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.

4 TERMINOLOGIA

1) **RODO** - Rozporządzenie 2016/679 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) **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Za osobę możliwą do zidentyfikowania przyjmuje się osobę, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności poprzez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.
3) **Zgoda osoby, której dane dotyczą** – rozumie się przez to oświadczenie woli, dobrowolne, konkretne, świadome i jednoznaczne lub jednoznaczne działanie potwierdzające osoby na przetwarzanie jej danych osobowych. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

4) **Przetwarzanie danych** – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, opracowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, a także dopasowywanie, łącznie, ograniczanie, usuwanie lub niszczenie.
5) **System informatyczny** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
6) **Naruszenie ochrony danych osobowych** – naruszenie bezpieczeństwa informacji, prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub przetwarzanych w inny sposób.
7) **Usuwanie danych** – rozumie się przez to trwałe zniszczenie danych osobowych.
8) **Anonimizacja danych** - przetworzenie danych osobowych w taki sposób, aby nie można ich było przypisać konkretnej osobie fizycznej, nawet przy zastosowaniu dodatkowych informacji. Modyfikacja danych osobowych, która nie pozwala na ustalenie tożsamości osoby, której dane dotyczą.
9) **Pseudonimizacja** – przetworzenie danych osobowych w taki sposób, by nie można ich było przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi, które uniemożliwiają przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.
10) **Administrator Danych (AD)** – administrator, rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 4, ust. 7 RODO, decydujący o celach i środkach przetwarzania danych osobowych.
11) **Administrator Systemu Informatycznego (ASI)** – osoba lub dział zajmujący się w szczególności nadzorowaniem pracy serwerów, zarządzaniem kontami użytkowników, konfiguracją komputerów, instalowaniem oprogramowania, dbaniem o bezpieczeństwo systemu i opcjonalnie samych danych, nadzorowanie, wykrywanie i eliminowanie nieprawidłowości, asystowaniem i współpracą z zewnętrznymi specjalistami przy pracach instalacyjnych, konfiguracyjnych i naprawczych oraz innych zadań wynikających z zaleconych obowiązków.
12) **Inspektor Ochrony Danych (IOD)** - osoba nadzorująca z upoważnienia AD przestrzeganie obowiązujących przepisów o ochronie danych osobowych oraz stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych w sposób odpowiedni do zagrożeń oraz kategorii danych objętych ochroną, zgodnie z obowiązkami określonymi w art. 37-39 RODO.
13) **Członkowie organów statutowych Spółdzielni** – przez to sformułowanie w niniejszej Polityce rozumie się członków Rady Nadzorczej oraz Zarządu.
14) **Odbiorca danych** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawniane są dane osobowe, niezależnie od tego, czy jest stroną trzecią, z wyłączeniem organów publicznych lub podmiotów, w stosunku do których ujawnianie danych osobowych realizowane jest w ramach konkretnego postępowania zgodnie z prawem Unii lub państwa członkowskiego.
15) **Organ nadzorczy** – niezależny organ publiczny ustanowiony przez państwo monitorujący przestrzeganie przepisów o ochronie danych osobowych w danym państwie w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem i swobodnym przepływem danych osobowych.
16) **PUODO** – Prezes Urzędu Ochrony Danych Osobowych, organ nadzorczy w Polsce.
17) **UODO –** Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.
18) **Konsultacje** – uprzednie konsultacje z PUODO dokonywane w przypadku, o którym mowa w art. 36 ust. 1 RODO obejmującym przypadek, gdy ocena skutków przetwarzania (DPIA) wskazuje, że przetwarzanie danych osobowych powodowałoby wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą gdyby Administrator nie zastosował środków technicznych i organizacyjnych w celu zminimalizowania tego ryzyka lub po wdrożeniu tych środków poziom ryzyka nie uległ zmianie, a Administrator zamierza dokonywać przetwarzania danych osobowych w ramach tej czynności przetwarzania.

19) **Kontrolujący** – osoba prowadząca postępowanie kontrolne przestrzegania przez Administratora przepisów o ochronie danych osobowych zgodnie z UODO.
20) **Użytkownik systemu** – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych zarejestrowaną w systemie informatycznym AD.
21) **Sieć lokalna** – należy przez to rozumieć połączenie systemów informatycznych AD wyłącznie dla jego własnych potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych.
22) **Sieć publiczna** – należy przez to rozumieć publiczną sieć telekomunikacyjną w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne.
23) **Użytkownik zdalny** - użytkownik systemu łączący się z sieci rozległej z systemem informatycznym AD znajdującym się w sieci lokalnej, lub pracujący zdalnie na danych poza siedzibą AD.
24) **Program komputerowy** – zbiór instrukcji, które po umieszczeniu na rozpoznawalnym przez maszynę nośniku i automatycznym przetłumaczeniu na język zrozumiały dla tej maszyny powoduje, że osiąga on zdolność do wykonywania danej czynności lub też wykonuje daną czynność.
25) **Serwer** - wyróżniony komputer świadczący usługi na rzecz mających z nim łączność innych komputerów np. przechowujący pliki, pośredniczący w przekazywaniu poczty itp.
26) **Baza danych** - zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych np. w pamięci zewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze rekordów lub obiektów, w których są zapisane dane jednostkowych obiektów.
27) **Kopie bezpieczeństwa (zapasowe)** – kopie plików danych lub plików programowania tworzone na nośniku wymiennym lub dysku twardym komputera w celu ich odtworzenia w przypadku utraty lub uszkodzenia danych.
28) **Teletransmisja (przesyłanie) danych** - przesyłanie danych przy pomocy dostępnych łączy.
29) **Plik** – nośnik informacji, ciąg bajtów posiadający swoją nazwę odróżniającą ją od innych plików i parametry: rozmiar, datę powstania lub datę ostatniej modyfikacji itp.
30) **Nośnik komputerowy (wymienny, lub pamięć/nośnik przenośny)** – nośnik służący do zapisu informacji, np. płyta CD, wymienny dysk twardy, pamięć typu „pendrive" lub jakakolwiek inna forma pamięci nadająca się do przenoszenia danych (np. pamięć w urządzeniach tj. smartphone).
31) **Szkodliwe oprogramowanie** – (np. tzw. wirus, koń trojański itd.) program, który uaktywniony w pamięci operacyjnej, powoduje wadliwe działanie, zniszczenie lub modyfikację systemu operacyjnego, programu komputerowego lub danych, program, który udaje pracę innego legalnego programu, a w międzyczasie wykonuje szereg niepożądanych czynności (np. fałszywy program „login" kradnie hasło użytkownika).

W zakresie terminologii nieuregulowanej niniejszą **Polityką** mają zastosowanie definicje wskazane w art. 4 RODO.

5 ORGANIZACJA PRZETWARZANIA DANYCH OSOBOWYCH

5.1 ADMINISTRATOR DANYCH

Do zadań Administratora Danych (AD), należy:

- podział zadań i obowiązków związanych z organizacją ochrony danych osobowych wśród pracowników;
- podjęcie decyzji o wyznaczeniu Inspektora Ochrony Danych (IOD);
- podejmowanie decyzji o celach i środkach przetwarzania danych osobowych, zwłaszcza z uwzględnieniem zmian w obowiązujących przepisach prawa, regulacji wewnętrznych oraz technik zabezpieczenia danych osobowych;

- zawiadomienie PUODO o wyznaczeniu, zmianie, odwołaniu lub zmianie danych kontaktowych IOD oraz o zmianie danych kontaktowych AD (np. zmianie siedziby Spółdzielni);
- podejmowanie odpowiednich działań w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa danych osobowych, w szczególności obejmujących zgłaszanie naruszenia do organu nadzorczego, do PUODO i dokonywanie zawiadomień osób, których dane dotyczą, o naruszeniu ich danych osobowych;
- wydawanie upoważnień do przetwarzania danych osobowych dla wszystkich osób mających dostęp do danych osobowych przetwarzanych w Spółdzielni. Upoważnienia wydawane są przez AD lub przez osobę posiadającą pełnomocnictwo AD;
- wdrażanie wewnętrznych procedur i regulacji dotyczących ochrony danych osobowych;
- regularna ocena ryzyka oraz ocena skutków przetwarzania danych osobowych;
- prowadzenie uprzednich konsultacji z organem nadzorczym w rozumieniu art. 36 RODO;
- prowadzenie rejestru czynności i rejestru kategorii czynności przetwarzania w rozumieniu art. 30 RODO;
- przeprowadzanie testów równowagi;
- zapewnienie niezbędnych środków w celu zapewnienia bezpieczeństwa przetwarzanych danych osobowych;
- wypełnienie obowiązków informacyjnych na mocy art. 13-14 RODO.

AD zobowiązany jest również do dołożenia wszelkich starań związanych z ochroną danych osobowych dotyczących:

a) podejmowania działań wskutek stwierdzonych naruszeń ochrony danych osobowych;
b) umożliwienia osobom, których dane dotyczą, realizację praw na mocy art. 15-22 RODO;
c) wdrażanie środków techniczno-organizacyjnych i wszelkich innych zabezpieczeń, aby przetwarzanie danych osobowych odbywało się zgodnie przepisami o ochronie danych osobowych, w tym w szczególności dokonywać przeglądu wdrożonych zabezpieczeń oraz dokonywać ich aktualizacji/zmiany pod katem zwiększenia bezpieczeństwa przetwarzania danych osobowych

W tym zakresie AD powinien uwzględniać:

- charakter, zakres, kontekst, cele przetwarzania oraz ryzyko naruszenia praw i wolności osób;
- stan wiedzy technicznej, koszt wdrażania odpowiednich środków;
- zastosowanie metod pseudonimizacji i szyfrowania danych osobowych;
- zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
- regularne testowanie, mierzenie i ocenianie skuteczności wdrożonych zabezpieczeń zarówno fizycznych jak i teleinformatycznych.

5.2 INSPEKTOR OCHRONY DANYCH

Do zadań Inspektora Ochrony Danych należy:

- informowanie AD oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy przepisów o ochronie danych osobowych i doradzanie im w tej sprawie;
- monitorowanie przestrzegania przepisów o ochronie danych osobowych oraz polityk AD w dziedzinie ochrony danych osobowych, w tym przeprowadzanie sprawdzeń;
- prowadzenie działań zwiększających świadomość pracowników w dziedzinie ochrony danych osobowych, w szczególności szkoleń personelu uczestniczącego w operacjach przetwarzania;
- wsparcie AD w procesie udostępniania danych osobowych i realizacji praw osób, których dane dotyczą;
- wsparcie AD w tworzeniu i aktualizacji dokumentacji przetwarzania danych osobowych;
- wsparcie w prowadzeniu i corocznym przeglądzie rejestru czynności przetwarzania;

- wsparcie w prowadzeniu rejestru naruszeń ochrony danych osobowych i monitorowania ryzyka naruszenia praw i wolności osób, których dane dotyczą, w szczególności przekazywanie rekomendacji co do postępowania z naruszeniem i zawiadomienia organu nadzorczego;
- udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;
- wydawanie wytycznych i rekomendacji dla procesów, w których przetwarzane są dane osobowe;
- przeprowadzanie analizy przypadków stwierdzonych lub podejrzewanych o naruszenie bezpieczeństwa danych osobowych oraz przedstawianie raportu i zaleceń dla AD w tym zakresie;
- współpraca z organem nadzorczym (w Polsce: z PUODO) i pełnienie funkcji punktu kontaktowego dla organu nadzorczego.

W zakresie wykonywanych czynności IOD przekazuje roczny plan działań planowanych w zakresie ochrony danych osobowych, w tym planowane sprawdzenia u AD. IOD może również dokonywać sprawdzenia doraźnego mającego charakter niezapowiedzianej wizyty, w szczególności w oparciu o stwierdzone naruszenia ochrony danych osobowych, zmianę przepisów prawa, komunikaty PUODO lub wystąpienie innych okoliczności mających wpływ na bezpieczeństwo przetwarzanych danych przez AD oraz ryzyko naruszenia praw i wolności osób, których dane dotyczą. W przypadku wykonywania sprawdzenia, IOD dokumentuje czynności objęte sprawdzeniem w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz do opracowania sprawozdania.
W przypadku wykrycia nieprawidłowości, IOD zawiadamia o tym AD lub upoważnionego pracownika w formie pisemnej, najczęściej w formie pisemnego raportu ze sprawdzenia, notatki z wizyty. IOD wydaje w tym zakresie wytyczne, zalecenia i rekomendacje do wdrożenia. Decyzję co do zasadności rekomendacji oraz podjęcie decyzji o wdrożeniu i usunięciu nieprawidłowości podejmuje AD.

5.3 ADMINISTRATOR SYSTEMU INFORMATYCZNEGO

Do zadań Administratora Systemu Informatycznego (ASI) należy w szczególności:

- przeciwdziałanie dostępowi osób nieupoważnionych do systemu informatycznego, w którym przetwarzane są dane osobowe, w ramach posiadanych uprawnień;
- branie udziału w cyklicznych działań związanych z przeprowadzaniem oceny ryzyka na wniosek AD;
- na wniosek przełożonego osoby przydzielenie każdemu użytkownikowi identyfikatora i hasła oraz nadawanie, modyfikacja oraz odbieranie uprawnień;
- nadzorowanie działania mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do systemów służących do przetwarzania danych osobowych;
- nadzór i dbanie o bezpieczeństwo systemów teleinformatycznych Administratora;
- podejmowanie działań służących zapewnieniu niezawodności działania komputerów i innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji;
- ASI odpowiada za bezpieczeństwo systemów teleinformatycznych wykorzystywanych przez Administratora.

5.4 KIEROWNICY DZIAŁÓW, KOMÓREK ORGANIZACYJNYCH LUB PRZEŁOŻENI OSÓB NA STANOWISKACH SAMODZIELNYCH:

Do zadań Kierowników działów należy:

- występowanie do ASI z wnioskami o nadanie uprawnień w systemie informatycznym dla podległych pracowników;
- podjęcie decyzji co do konieczności przetwarzania przez osoby danych osobowych i występowanie do AD lub jego upoważnionego przedstawiciela z wnioskiem o nadawanie lub odwołanie upoważnienia do przetwarzania danych osobowych;

- zgłaszanie naruszeń lub podejrzeń naruszeń ochrony danych osobowych do IOD, a jeżeli naruszenie lub podejrzenie dotyczy systemu informatycznego, zgłaszanie również tego faktu ASI;
- występowanie do IOD z wnioskiem o przeszkolenie pracowników z zasad ochrony danych osobowych;
- zapewnienie zapoznania podległych pracowników z wewnętrznymi regulacjami dotyczącymi ochrony danych, w tym aktualną wersją niniejszego dokumentu;
- udział w procesie odpowiadania na żądania osób, których dane dotyczą zgodnie z uprawnieniami osób przewidzianymi w art. 15-22 RODO;
- udział w procesie udostępniania danych osobowych na żądanie odbiorcy i weryfikacji udostępnianych danych;
- bieżąca weryfikacja przestrzegania przez podległych pracowników przyjętych zasad przetwarzania danych osobowych.

5.5 OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH

Do obowiązków wszystkich osób upoważnionych do przetwarzania danych osobowych należy:

- przetwarzanie danych wyłącznie w takim zakresie i w takim celu, jaki wynika bezpośrednio z obowiązków służbowych oraz nadanego upoważnienia do przetwarzania danych osobowych;
- przestrzeganie przepisów o ochronie danych osobowych oraz przyjętych w Spółdzielni zasad przetwarzania danych osobowych, w tym zachowanie poufności i nieujawnianie osobom, stronom trzecim żadnych informacji, z jakimi zapoznały się w związku z pełnionymi obowiązkami służbowymi, w tym danych uwierzytelniających (np. haseł, loginów);
- dbałość o bezpieczeństwo nośników i urządzeń służących do przetwarzania danych zarówno w siedzibie Spółdzielni jak i poza nią;
- zgłaszanie wszystkich podejrzanych lub faktycznych nieprawidłowości w procesie przetwarzania danych kierownikowi działu oraz do IOD,
- postępowanie zgodnie z wewnętrznymi regulacjami dotyczącymi przetwarzania danych osobowych w szczególności dotyczących zabezpieczenia danych i nośników danych osobowych opisanych w **Podręczniku bezpieczeństwa**.

Specjalista ds. Kadr prowadzi **Rejestr osób upoważnionych** do przetwarzania danych osobowych, gdzie upoważnienia te zostały wydane przez Zarząd lub jego upoważnionego przedstawiciela.

5.6 SZKOLENIA Z OCHRONY DANYCH OSOBOWYCH

Każda osoba, która przetwarza dane osobowe (nawet poddane pseudonimizacji) zobowiązana jest do odbycia szkolenia z ochrony danych osobowych. Szkolenie przeprowadzane jest w formie ustalonej z AD, np. instruktażu stanowiskowego przez IOD lub w formie e-learningowej. Informacjami potwierdzającymi szkolenie może być: podpis na liście obecności ze szkolenia, log z platformy szkoleniowej o uzyskaniu pozytywnego wyniku, notatka ze szkolenia lub inna forma, która jednoznaczny potwierdzi uczestnictwo w szkoleniu.
Kierownik działu/jednostki lub bezpośrednio AD zobowiązani są do niezwłocznego poinformowania IOD o konieczności przeszkolenia nowego pracownika. Ponadto każdemu nowemu pracownikowi udostępniana jest **Prezentacja szkoleniowa z ochrony danych osobowych.**

6 PRZETWARZANE DANE OSOBOWE

Wykaz przetwarzanych danych osobowych znajduje się w **Rejestrze czynności przetwarzania.** Za obszar przetwarzania danych osobowych uznaje się cały obszar Administratora Danych. Wykaz kategorii przetwarzanych danych osobowych (jako podmiot przetwarzający) wskazano w **Rejestrze kategorii czynności przetwarzania**.

W stosunku do danej czynności przetwarzania danych osobowych, AD dokonuje przetwarzania na podstawie odpowiedniej podstawy prawnej, również z uwzględnieniem, czy dochodzi do przetwarzania danych osobowych szczególnej kategorii, w odniesieniu do art. 6 RODO oraz art. 9 RODO.

W przypadku przetwarzania danych osobowych w oparciu o prawnie uzasadniony interes AD (art. 6 ust. 1 lit. f RODO) lub strony trzeciej, z wyjątkiem sytuacji, gdy nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą wymagające ochrony danych osobowych – w tym zakresie AD lub osoba przez niego wyznaczona przeprowadza **Testy równowagi**, w szczególności przed rozpoczęciem przetwarzania danych osobowych.

6.1 ZASADY WYRAŻANIA I WYCOFYWANIA ZGODY

AD dokonuje wszelkich starań, aby przetwarzanie danych osobowych na podstawie zgody zostało dokonywane w sposób niebudzący wątpliwości co do faktu jej wyrażenia. W zakresie wyrażania przez osoby zgody przyjmuje się następujące podstawowe zasady:

a) Zgoda powinna być wyrażona w drodze jednoznacznej, potwierdzającej czynności, w tym może stanowić jednoznaczne działanie potwierdzające dokonane przez osobę, której dane dotyczą. AD przedstawia osobie, której dane dotyczą informację odnośnie przetwarzania danych osobowych zgodnie z art. 13 RODO.

b) Zgoda powinna odnosić się do określonej sytuacji i powinna być wyrażana w sposób jednoznaczny i dobrowolny m.in. poprzez:
- Wypełnienie stosownego pisemnego oświadczenia w formie papierowej lub elektronicznej;
- Zaznaczenie okienka wyboru (typu checkbox);
- Wybór odpowiednich ustawień technicznych do korzystania z usług społeczeństwa informacyjnego;
- Dodanie do przekazywanych dokumentów określonych przez AD klauzul zgód;
- Inne oświadczenie bądź zachowanie, które w danym kontekście jasno wskazuje, że osoba, której dane dotyczą, zaakceptowała proponowane przetwarzanie jej danych osobowych.

c) Milczenie, okienka domyślnie zaznaczone lub niepodjęcie działania nie oznaczają zgody.

d) Zgoda powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach.

e) Oświadczenie o wyrażeniu zgody przygotowane przez AD powinno mieć zrozumiałą i łatwo dostępną formę, być sformułowane jasnym i prostym językiem i nie powinno zawierać nieuczciwych warunków.

f) Jeżeli przetwarzanie służy różnym celom, potrzebna jest zgoda na wszystkie te cele, w formie odrębnych zapytań lub oświadczeń. Łączenie różnych celów przetwarzania w formie jednego oświadczenia bez dania wyboru, na który z podanych wariantów osoba, której dane dotyczą się zgadza jest działaniem nieprawidłowym.

g) Zgody nie uważa się za dobrowolną, jeżeli nie można jej wyrazić z osobna na różne operacje przetwarzania danych osobowych, mimo że w danym przypadku byłoby to stosowne, lub jeżeli od zgody uzależnione jest wykonanie umowy – w tym świadczenie usługi – mimo że do jej wykonania zgoda nie jest niezbędna.

h) Wyrażenia zgody nie uznaje się za dobrowolne, jeżeli osoba, której dane dotyczą, nie ma rzeczywistego lub wolnego wyboru oraz nie może odmówić ani wycofać zgody bez niekorzystnych konsekwencji.

AD przed rozpoczęciem przetwarzania, w celu zapewnienia dobrowolności wyrażenia zgody, dokonuje weryfikacji procesów przetwarzania, aby zgoda nie stanowiła ważnej podstawy prawnej przetwarzania danych osobowych w szczególnej sytuacji, w której istnieje wyraźny brak równowagi między osobą, której dane dotyczą, a AD.

Do mechanizmów wycofania zgody AD stosuje m.in.:

1) formę papierową (w przypadku oświadczeń zgód pobieranych w formie papierowej);
2) formę elektroniczną (np. odznaczenie okienka zgody, przekazanie zgłoszenia wycofania zgody na adres sekretariat@smkozlowek.krakow.pl lub inny wskazany w treści zgody lub treści obowiązku informacyjnego).

Informacje dotyczące mechanizmów wycofywania zgody stanowią jeden z elementów klauzul informacyjnych lub polityk prywatności, w zależności od procesu przetwarzania.

6.2 WYKONYWANIE PRZEGLĄDÓW I USUWANIE LUB ANONIMIZACJA DANYCH OSOBOWYCH

Kierownicy działów/jednostek odpowiedzialni są za bieżący nadzór nad przetwarzaniem danych w podległym obszarze przez okres przyjęty w **Rejestrze czynności przetwarzania**.

Każdy dział / jednostka przynajmniej raz w roku dokonuje weryfikacji przetwarzanych danych osobowych. Przegląd danych obejmuje dokumenty elektroniczne, papierowe oraz informacje zawarte w systemach informatycznych wykorzystywanych przez AD. Osoby merytorycznie odpowiedzialne za dany proces podejmują decyzję co do zasadności pozostawienia, usunięcia lub anonimizacji danych osobowych.

W Spółdzielni przyjęto następujące zasady retencji danych osobowych:

1) Spółdzielnia dokonuje przetwarzania danych osobowych w formie umożliwiającej identyfikację podmiotu danych przez okres nie dłuższy, niż jest to konieczne do celów, w których te dane osobowe są przetwarzane, gdzie okres ten może być również wskazany przez przepisy obowiązującego prawa.
2) W przypadku, gdy dla określonych danych osobowych nie występują żadne prawnie uzasadnione interesy i cele przetwarzania, AD zaprzestaje realizowania jakichkolwiek operacji na tych danych (np. przechowywania, modyfikowania, gromadzenia, pobierania, wysyłania itp.), z wyjątkiem ich usunięcia lub nieodwracalnej anonimizacji.
3) W sytuacji, gdy okres retencji danych nie jest wskazany bezpośrednio w przepisie prawa, do AD należy ustalenie samodzielnie tego okresu uwzględniając zasady przetwarzania danych osobowych określonych w RODO:
   - **zgodność z prawem, rzetelność i przejrzystość**;
   - **ograniczenie celu przetwarzania** – zbieranie danych osobowych w konkretnych, wyraźnych oraz prawnie uzasadnionych celach i przetwarzane wyłącznie przez wymagany okres do wypełnienia tych celów i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
   - **ograniczenie przechowywania** – przechowywanie danych osobowych w formie umożliwiającej identyfikację osoby fizycznej przez okres nie dłuższy niż niezbędny do osiągnięcia celu przetwarzania, który wskazano w **Rejestrze czynności przetwarzania**;
   - **zapewnienie integralności i poufności** – zapewnienie odpowiedniego bezpieczeństwa danych osobowych, w tym ochrony przed niedozwolonym lub niezgodnym z prawem przetwarzaniem, a także przypadkową utratą, zniszczeniem, uszkodzeniem, za pomocą odpowiednich zabezpieczeń obejmujących środki fizyczne, techniczne, organizacyjne;
   - **minimalizacja danych** – określenie danych niezbędnych do wypełnienia celu przetwarzania, stosowanie zasady adekwatności danych osobowych, stosownych i ograniczonych do tego co jest niezbędne do wypełnienia celu przetwarzania, brak gromadzenia danych nadmiarowych;
   - **prawidłowość danych** – zapewnienie możliwości aktualizacji danych, przetwarzanie danych zgodnych ze stanem faktycznym, podjęcie wszelkich rozsądnych działań, aby nieprawidłowe dane osobowe zostały niezwłocznie usunięte lub sprostowane.
4) W sytuacji, gdy okres retencji wynika bezpośrednio z przepisów prawa, AD dokonuje przetwarzania danych przez okres nie krótszy niż określony w tych przepisach.
5) Przy ustalaniu okresu retencji danych brane są również pod uwagę prawnie uzasadnione interesy AD związane w szczególności z ustaleniem, dochodzeniem i obroną przed roszczeniami oraz związane z nimi okresy przedawnienia tych roszczeń, w zależności od rodzaju roszczenia i prowadzonego postępowania, co wynika z właściwych przepisów obowiązującego prawa.
6) Okresy retencji danych osobowych określone w **Rejestrze czynności przetwarzania** mogą ulegać zmianie w związku ze zmianą przepisów prawa, w których określone są terminy przetwarzania danych lub w związku z decyzją AD podjętą wobec

danego celu przetwarzania, o czym osoby zatrudnione w Spółdzielni są informowane, a w przypadku, gdy jest to uzasadnione – również osoby, których dane dotyczą.

7) Przed usunięciem danych osobowych lub ich anonimizacją należy zweryfikować, czy nie zachodzą przesłanki wydłużenia okresu retencji, tj. weryfikacja czy:
   - konkretny przepis prawa wskazuje AD na obowiązek dalszego przetwarzania, a przepis ten nie został uwzględniony w **Rejestrze czynności przetwarzania;**
   - nie nastąpiło przerwanie lub zawieszenie okresu przedawnienia roszczeń, w zależności od rodzaju roszczenia, jego terminu, zgodnie z przepisami prawa, które skutkują koniecznością dalszego przetwarzania danych osobowych;
   - dalsze przechowywanie nie jest konieczne z punktu widzenia okresu przedawnienia roszczeń wynikających z zobowiązań podatkowych i przepisów podatkowo-rachunkowych z tym związanych.
8) Przed usunięciem lub anonimizacją danych kierownik działu/jednostki lub osoba przez niego wyznaczona może zwrócić się do IOD o opinię w przedmiotowej sprawie.
9) Usunięcie lub anonimizacja danych powinna nastąpić niezwłocznie po upływu okresu retencji, z uwzględnieniem okresu niezbędnego do podjęcia odpowiednich czynności technicznych i organizacyjnych przez pracowników w związku z dokonywanym przeglądem danych osobowych i podjęciem decyzji o ich usunięciu lub anonimizacji. Czynności te mogą dotyczyć m.in. określenia:
   - metod dokonywania przeglądu oraz osób odpowiedzialnych;
   - grupy dokumentów objętych przeglądem lub grupy danych osobowych;
   - określenia systemów informatycznych podlegających przeglądowi i formy dokumentowania wyników tego przeglądu;
   - formy dokonywania wyników przeglądu oraz decyzji podjętej w wyniku przeglądu (usunięcia, anonimizacji lub pozostawienia danych osobowych).

W przypadku, gdy w ocenie AD przeglądany dokument elektroniczny lub papierowy powinien być nadal przechowywany, lecz nie jest niezbędne przetwarzanie danych osobowych, AD może dokonać anonimizacji danych osobowych na tym dokumencie. Anonimizacja powinna zapewniać trwałe usunięcie danych osobowych, bez możliwości ich dalszego odtworzenia. Do metod anonimizacji mogą należeć:

a) zaczernienie danych osobowych (np. flamaster, przy użyciu specjalistycznego oprogramowania) w formie nieodwracalnej (tj. bez możliwości „odsłonięcia" zaczernionych danych);
b) zastąpienie danych znakiem wodnym, obrazkiem lub inicjałami;
c) zastąpienie danych w systemie informatycznym innymi danymi, losowo wygenerowanymi, które nie są powiązane w żaden sposób z danymi osobowymi uprzednio zawartymi w systemie, nawet przy użyciu dodatkowych środków (np. zestawienia baz danych, użycia klucza deszyfrującego);
d) metody statyczne, m.in.
   - randomizacja, czyli losowy rozdział danych w celu wyeliminowania ścisłego związku między danymi a konkretną osobą fizyczną;
   - generalizacja (uogólnienie), czyli celowe obniżenie precyzji danych (np. zmiana dokładnego wieku osoby na przedział wiekowy);
   - supresja atrybutów, czyli usunięcie całej partii danych (w arkuszach i bazach danych nazywanej również "kolumną") w zestawie danych;
   - supresja rejestrów, czyli całego rejestru w zestawie danych. W odróżnieniu od innych technik, ta metoda wpływa na wiele zmiennych jednocześnie.

W przypadku, gdy zastosowana technika umożliwia, przy użyciu dodatkowych środków (np. zestawienia informacji z inną bazą danych, dokumentem) identyfikację bezpośrednią lub pośrednią osoby fizycznej, uznaje się, że doszło do pseudonimizacji, a nie anonimizacji danych i należy zastosować inną technikę.

Dokonując anonimizacji dokumentu należy pozbawić go informacji, które powodują, że daną osobę fizyczną można zidentyfikować, np. nr PESEL, NIP, wizerunku, adresie, numerze telefonu.

Kierownik działu/jednostki może wyznaczyć osobę lub zespół osób bezpośrednio odpowiedzialnych za nadzór nad przetwarzanymi danymi osobowymi, w szczególności za przegląd danych osobowych pod kątem ich adekwatności i podjęcie decyzji o pozostawieniu tych danych lub ich usunięciu, lub anonimizacji.

Jeżeli podjęto decyzje o wykonaniu corocznego przeglądu przez każdy dział lub wykonanie tego przeglądu jest wymaganiem przepisu prawa, przegląd taki jest dokumentowany w postaci raportu, notatki lub w innej, pisemnej formie (np. log z systemu, gdy dokonano usunięcia lub ograniczenia danych osobowych).

Ponadto w związku z art. Art. 8[1] ust. 3 ustawy z dnia 15 grudnia 2000 r. o spółdzielniach mieszkaniowych AD przyjmuje zasadę, iż publikacja uchwał i protokołów organów Spółdzielni, może zostać udostępniona w wydzielonym module na stronie internetowej wyłącznie po uprzedniej anonimizacji danych osobowych, obejmujących m.in. dane osób posiadających tytuł prawny do lokalu, dane członków spółdzielni, dane osób zalegających w płatnościach na rzecz AD, dane najemców i dzierżawców oraz dane innych osób trzecich. Anonimizacja nie obejmuje danych osobowych członków organów statutowych Spółdzielni ani protokołów obrad Walnego Zgromadzenia Członków Spółdzielni. Uchwały i protokoły organów statutowych publikowane są na stronie internetowej AD w wydzielonym module, do którego dostęp posiadają wyłącznie członkowie Spółdzielni po uwierzytelnieniu za pośrednictwem loginu i hasła dostępowego. Login i hasło wydawane są przez uprawnionego pracownika osobiście członkowi Spółdzielni po dokonaniu weryfikacji tożsamości oraz uprawnień do uzyskania dostępu do modułu. W przypadku publikacji protokołu obrad Walnego Zgromadzenia Członków Spółdzielni na ogólnodostępnej stronie internetowej AD podlega on anonimizacji.

W ramach swoich uprawnień Członek Spółdzielni ma prawo otrzymywania kopii uchwał i protokołów organów Spółdzielni, kopie te wydawane są jedynie na pisemny wniosek członka wyłącznie po uprzedniej anonimizacji danych osobowych. Szczegółowy tryb sporządzania odpisów oraz kopii uchwał i protokołów organów statutowych jest uregulowany w odpowiednim regulaminie wewnętrznym Administratora.

7 PROJEKTOWANIE PROCESÓW PRZETWARZANIA I DOMYŚLNEJ OCHRONY DANYCH OSOBOWYCH

Do zadań AD należy kształtowanie odpowiedniego poziomu ochrony danych osobowych wśród pracowników, osób wykonujących pracę na rzecz AD oraz osób obecnych na terenie AD lub korzystających z jego zasobów. Przed rozpoczęciem przetwarzania danych osobowych AD zobowiązany jest do przeanalizowania czy na etapie projektowania uwzględniono zasady ochrony danych osobowych, w szczególności:

- czy dokonano oszacowania, jakich kategorii osób będzie dotyczyło przetwarzanie;
- czy dokonano oszacowania, jakich kategorii danych będzie dotyczyło przetwarzanie (w szczególności, czy przetwarzaniu będą podlegać dane osobowe szczególnej kategorii);
- czy dokonano oszacowana niezbędnego zakresu danych, które mają być przetwarzane w ramach danej czynności przetwarzania w stosunku do kategorii gromadzonych danych osób;
- czy określono cel przetwarzania danych osobowych;
- czy oszacowano, czy będzie wykonywany proces profilowania i zautomatyzowany proces podejmowania decyzji;
- czy określono podstawę prawną uprawniającą do takiego przetwarzania danych, a gdy przetwarzanie ma być realizowane w oparciu o prawnie uzasadniony interes Administratora Danych (art. 6 ust. 1 lit. f RODO) – czy wykonano **test równowagi**;
- czy określono, jakie podmioty będą uczestniczyły w procesie przetwarzania i jaka jest ich rola w tym procesie;
- czy określono, czy przetwarzanie będzie realizowane w państwach trzecich;
- czy określono odpowiednie środki techniczne i organizacyjne i zasady pseudonimizacji w celu gromadzenia wyłącznie niezbędnego, minimalnego zakresu danych osobowych w ramach danej czynności bez względu, czy dane przetwarzane będą w

formie papierowej czy w formie elektronicznej, w systemach teleinformatycznych (obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności);

- czy wdrożone zabezpieczenia zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób, w tym również pracownikom i podwykonawcom i zleceniobiorcom.

W celu odpowiedniej weryfikacji procesu, AD zobowiązany jest do przeprowadzania analiz projektowanych procesów przetwarzania danych osobowych przed rozpoczęciem przetwarzania. W przypadku, gdy planowane operacje przetwarzania mogą powodować wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą, AD zobowiązany jest do wykonania **oceny skutków dla ochrony danych**. Zarówno podczas projektowania procesów ochrony danych i zapewnienia zasad domyślnej ochrony danych, w projektowanie procesu i analizę ewentualnych ryzyk, powinni być zaangażowani pracownicy odpowiadający za proces przetwarzania danych osobowych, w szczególności kierownicy danych działów, pracownicy firm zewnętrznych np. programiści (w przypadku aplikacji), ASI (w zakresie zabezpieczenia komponentów infrastruktury teleinformatycznych) oraz pracownicy innych działów/jednostek, w zależności od procesu, którzy istotnie wpływają na projektowany proces przetwarzania danych osobowych.

AD może na etapie projektowania procesu konsultować się z IOD. W przypadku oceny skutków dla ochrony danych, która wskazuje wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą, AD konsultuje ocenę z IOD. IOD wydaje na żądanie zalecenia i rekomendacje oraz monitoruje wykonanie takiej oceny przed rozpoczęciem przetwarzania. IOD może również zalecić uprzednie konsultacje z organem nadzorczym przed rozpoczęciem przetwarzania.

AD zobowiązany jest do informowania IOD o wszystkich sprawach dotyczących ochrony danych osobowych, w szczególności:

a) planowaniu wdrożenia nowych procesów związanych z przetwarzaniem danych osobowych;
b) modyfikacji procesów realizowanych na danych osobowych, w szczególności związanych z zakresem danych osobowych przetwarzanych w ramach procesu oraz uprawnieniami pracowników;
c) wdrożenia / zakupu komponentów infrastruktury, również teleinformatycznej, w których będą przetwarzane dane osobowe;
d) zmian kluczowych dostawców, np. dostawca systemu teleinformatycznego;
e) naruszeniach oraz podejrzeniach naruszeń związanych z ochroną danych osobowych, w tym również, jeśli naruszenie miało związek z funkcjonowaniem komponentów infrastruktury informatycznej i złamaniem zabezpieczeń;
f) naruszeniach ochrony danych osobowych podmiotu przetwarzającego (jeśli podmiot zawiadomił AD o takim naruszeniu na inny adres niż adres kontaktowy IOD).

AD powinien zapewnić IOD niezależność w wykonywanych przez niego zadaniach oraz niezbędne zasoby.

8 UDOSTĘPNIANIE DANYCH OSOBOWYCH

AD udostępnia dane osobowe przetwarzane we własnych zbiorach tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa lub na podstawie zgody właściciela danych. Dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że odrębne przepisy prawa stanowią inaczej. Wniosek powinien zawierać następujące informacje:

1. Odbiorcę danych – wnioskodawca;
2. Podstawę do uzyskania informacji (zgoda, przepis prawa);
3. Informację dotyczącą właściciela danych;
4. Zakres wymaganych informacji zgodny z uzyskaną zgodą lub przepisem prawa;
5. Cel uzyskania informacji.

Wniosek jest rozpatrywany przez AD lub upoważnionego przez niego pracownika. Osoba, która dokonała udostępnienia zachowuje wniosek i kopię pisma, w którym udostępniła dane do celów prawidłowego wykonania obowiązku informacyjnego wobec właściciela danych oraz do celów dowodowych.

AD może odmówić udostępnienia danych osobowych w następujących przypadkach:

1. Udostępnienie danych osobowych spowodowałoby istotne naruszenia dóbr osobistych osób, których dane dotyczą lub innych osób (z wyłączeniem sytuacji, w której do udostępnienia obliguje AD przepis prawa);
2. Dane osobowe nie mają istotnego związku ze wskazanymi we wniosku motywami działania Wnioskodawcy.

Przyjęta jest również zasada nieudzielania telefonicznie informacji o danych osobowych instytucjom, podmiotom zewnętrznym (np. bankom) oraz osobom trzecim bez uprzedniej weryfikacji tożsamości osoby dzwoniącej. Jeśli niemożliwa jest weryfikacji tożsamości – nie należy udzielać informacji o danych osobowych, które nie powinny być publicznie dostępnie – przez telefon, i należy poprosić Wnioskodawcę o pisemne złożenie wniosku o udostepnienie danych, na adres siedziby AD.

9 WYPEŁNIANIE OBOWIĄZKU INFORMACYJNEGO

Każda osoba, której dane zbiera bezpośrednio AD, musi zostać poinformowana w momencie zbierania tych danych o następujących informacjach:

- nazwie i adresie Administratora Danych (AD);
- danych kontaktowych Inspektora Ochrony Danych (IOD);
- celu i podstawie prawnej przetwarzania;
- ewentualnych odbiorcach danych;
- ewentualnym przekazaniu danych do państwa trzeciego;
- okresie w jakim dane będą przetwarzane;
- prawach przysługujących osobie (prawie dostępu do danych, do sprzeciwu i ewentualnego usunięcia oraz przenoszenia danych);
- prawie do wniesienia skargi do organu nadzorczego;
- obowiązku lub dobrowolności podania danych;
- ewentualnym zautomatyzowanym podejmowaniu decyzji w tym o profilowaniu (jeżeli dotyczy).

W przypadku pozyskania danych nie od osoby, której dane dotyczą, ale z innych źródeł, konieczne jest podanie także źródła pozyskania tych danych (chyba, że przepis prawa wyłącza taką możliwość). Informacji takich udziela się niezwłocznie po uzyskaniu danych, lecz najpóźniej niż podczas pierwszego kontaktu.

Każda osoba, której dane przetwarza Administrator danych ma prawo również uzyskać informacje o przetwarzaniu jego danych na żądanie. Odpowiedzi udziela się w terminie 30 dni. AD ma prawo odmówić udzielenia informacji, jeśli nie jest możliwe potwierdzenie tożsamości wnioskodawcy

Każda osoba, której dane przetwarza AD, ma prawo uzyskać powyższe informacje na żądanie. Odpowiedzi udziela się w terminie 30 dni. AD ma prawo odmówić udzielenia informacji, jeśli nie jest możliwe potwierdzenie tożsamości wnioskodawcy.

9.1 ZASADY WYPEŁNIANIA OBOWIĄZKÓW INFORMACYJNYCH

Przekazanie klauzuli informacyjnej może stanowić element formularza, umowy, regulaminu lub innego dokumentu, a także może stanowić odrębne oświadczenie przedstawiane osobom, od których zbierane są dane lub być dostępna w widocznym miejscu w momencie zbierania danych.

W przypadku pracowników AD wypełnienie obowiązku informacyjnego występuje w postaci przekazania klauzuli informacyjnej w postaci papierowych oświadczeń.

W przypadku kandydatów do pracy, oferentów, kontrahentów oraz innych stron zainteresowanych klauzula może być przekazywana w szczególności poprzez: pocztę elektroniczną (na wskazane adresy mailowe), bezpośrednie przekazanie w formie papierowej, w treści zamówienia lub specyfikacji przetargowej, w ramach aneksu do umowy lub zmiany obowiązującego dokumentu. Forma przekazania klauzuli dostosowywana jest indywidualnie.

10 REALIZACJA PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ, W TYM PRAWA DO SPRZECIWU, USUNIĘCIA, PRZENOSZENIA LUB UZYSKANIA KOPII DANYCH

Osobom przysługą prawa na mocy art. 15-22 RODO, tj.: prawo dostępu do danych, uzyskania kopii tych danych, sprostowania danych, usunięcia danych („prawo do bycia zapomnianym"), do ograniczenia przetwarzania, przenoszenia danych, sprzeciwu oraz do niepodlegania zautomatyzowanemu procesowi podejmowania decyzji i profilowaniu – chyba, że przepisy prawa stanowią inaczej.

Zgłoszenie realizacji prawa przysługuje wszystkim osobom fizycznym, których dane przetwarza AD, w tym również pracownikom.

Przyjmuje się następujące zasady postepowania:

1. Realizacja praw może nastąpić na pisemny (w tym elektroniczny) wniosek osoby przesłany przez wnioskodawcę na adres poczty elektronicznej: sekretariat@smkozlowek.krakow.pl lub w formie papierowej na adres korespondencyjny AD, bądź przekazany osobiście przez wnioskodawcę. Wniosek powinien zostać zarejestrowany w dzienniku podawczym AD.
2. Do przyjmowania zgłoszeń o realizację prawa można wykorzystywać druk **Zgłoszenia realizacji praw z ochrony danych osobowych.** Wnioski o realizację prawa złożone bez wypełnienia wniosku, lecz zawierające wszystkie wymagane dane, są również obsługiwane. Formularz ten jest dostępny dla stron zainteresowanych na ogólnodostępnej witrynie Spółdzielni, pod adresem: http://www.smkozlowek.krakow.pl/dokumenty/pozostale lub w formie papierowej w siedzibie AD.
3. Za obsługę zgłoszenia realizacji prawa odpowiadają kierownicy działów / jednostek lub osoby przez nich wyznaczone do tego celu, a w przypadku przetwarzania danych w systemach informatycznych – ASI.
4. Podczas oceny wniosku należy brać pod uwagę przede wszystkim to, czy:
   - Można ustalić i potwierdzić tożsamość wnioskodawcy;
   - Dane wnioskodawcy są przetwarzane w zasobach Spółdzielni;
   - Wniosek jest zasadny zgodnie z zapisami art. 16 – 19 RODO.
4. Jeżeli nie jest możliwa jednoznaczna identyfikacja należy niezwłocznie skontaktować się z osobą, której dane dotyczą w celu uzyskania dodatkowych danych identyfikujących osobę w bazach danych, dokumentach i systemach.
5. W przypadku, gdy nie można zagwarantować prawidłowej weryfikacji, można zażądać osobistego stawiennictwa osoby w siedzibie Spółdzielni w celu realizacji przysługującej jej praw – informacje te zostają przekazane wnioskodawcy w formie wskazanej przez wnioskodawcę, a w przypadku gdy nie wskazano tej formy – w takiej formie, w jakiej uzyskano zgłoszenie realizacji prawa.
6. Proces obsługi wniosku, na każdym jego etapie, można konsultować z IOD. IOD stanowi również merytoryczne wsparcie przy przekazywaniu osobom, których dane dotyczą, informacji związanych z żądaniem.
7. Odpowiedź dla osoby formułowana jest jasnym i prostym językiem w formie pisemnej, która konsultowana jest z IOD i przekazywana przez osobę odpowiedzialną za obsługę wniosku ze strony AD.
8. Jeżeli osoba, której dane dotyczą, zażąda udzielenia informacji w formie ustnej to przekazanie takich informacji może być zrealizowane wyłącznie w ustalonym przez obie strony terminie, w siedzibie AD lub siedzibie Administracji, gdzie z przebiegu takiego przekazania informacji sporządzana jest notatka.
9. **AD w terminie 30 dni od otrzymania żądania udziela osobie informacji o wszelkich podjętych działaniach w następstwie wniosku.**
10. W przypadku, gdy żądanie realizacji prawa jest skomplikowane (np. dane są rozproszone w systemach informatycznych), termin realizacji prawa może ulec wydłużeniu po uprzednim poinformowaniu wnioskodawcy wraz z powodem opóźnienia o kolejne dwa miesiące.
11. Jeżeli w ocenie AD złożony wniosek przez osobę nie wymaga podejmowania działań to również w terminie miesiąca od otrzymania żądania informuje on osobę o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych oraz skorzystania ze środków ochrony prawnej przed sądem.

Pierwszy wniosek realizowany jest bez opłat, lecz dopuszcza się możliwość naliczenia opłaty w przypadku, gdy żądania są nadmierne lub nieuzasadnione, np. w przypadku, gdy osoba wnioskująca wielokrotnie występuje z wnioskiem o udzielenie informacji lub o realizację praw w zakresie niewnoszącym zmian co do sposobu przetwarzania danych, AD informuje osobę wnioskującą o wysokości opłaty za udzielenie tych informacji. Jeżeli kontakt z osobą wnioskującą możliwy jest przy wykorzystaniu kanałów elektronicznych, kontakt z tą osobą może być prowadzony w ten sposób.

11 POWIERZENIE PRZETWARZANIA

Administrator Danych może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze **umowy zawartej w formie pisemnej**. Podmiot, któremu AD powierzył dane, jest zobowiązany do zastosowania środków organizacyjnych i technicznych, zabezpieczających zbiór przed dostępem osób nieupoważnionych na zasadach określonych w przepisach o ochronie danych osobowych oraz jest zobowiązany przetwarzać dane osobowe wyłącznie w zakresie, w jakim reguluje to zawarta umowa.

Zapisy w umowie z podmiotem, któremu powierzono przetwarzanie danych musi zawierać zapisy gwarantujące, co najmniej, że podmiot ten:

- przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora Danych;
- nie będzie podzlecał czynności jakie wykonuje dla Administratora Danych bez jego pisemnej zgody;
- zapewnia, by osoby upoważnione do przetwarzania danych osobowych po jego stronie zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
- wspomaga Administratora Danych w wykonywaniu obowiązku informacyjnego;
- zabezpiecza powierzone dane osobowe w sposób adekwatny do zagrożeń, w tym zgodnie z instrukcjami przekazanymi przez Administratora Danych;
- zabezpiecza, zwraca lub niszczy dane i nośniki po ustaniu świadczenia usług – zależnie od wzajemnych ustaleń;
- umożliwia Administratorowi Danych przeprowadzenie kontroli zgodności przetwarzania danych z umową.

W każdym przypadku, kiedy AD lub IOD uzna to za konieczne, można dokonać oceny podwykonawcy w celu weryfikacji spełnienia obowiązków wynikających z RODO oraz należytego wykonania zobowiązań. Ocenę podwykonawcy można wykonać poprzez:

- żądanie wyjaśnień i przedstawienia dowodów realizacji wymagań RODO;
- autoocenę podwykonawcy w oparciu o ankiety przygotowane przez AD;
- audyt drugiej strony, wykonany przez IOD lub osoby wskazane przez AD.

W celu oceny podwykonawcy AD może wykorzystać **Kwestionariusz oceny podmiotu**, w szczególności w stosunku do podmiotów, gdzie dochodzi do powierzenia przetwarzania danych osobowych szczególnej kategorii lub szerokiego zakresu danych. Decyzję w tym zakresie podejmuje AD.

12 BEZPIECZEŃSTWO PRZETWARZANIA DANYCH OSOBOWYCH

W celu zapewnienia poufności, integralności i rozliczalności przetwarzania danych AD stosuje środki techniczne i organizacyjne właściwe dla zapewnienia odpowiednich wymagań w zakresie bezpieczeństwa przetwarzania danych osobowych stosownie do wymogów określonych w art. 32 RODO oraz zgodnie z okresowo przeprowadzaną oceną ryzyka. Informacje dotyczące zasad postępowania dla pracowników zawarto w **Podręczniku bezpieczeństwa.**

12.1 ZABEZPIECZENIA FIZYCZNE OBSZARU BEZPIECZNEGO

AD stosuje zabezpieczenia pomieszczeń, biur, miejsc i nośników danych, bez względu na ich formę, które chronią przetwarzane dane przed dostępem osób nieupoważnionych. Do pomieszczeń, w których przetwarzane są dane osobowe dostęp mają wyłącznie osoby posiadające upoważnienie od AD. Zasady ochrony fizycznej dla pracowników opisane są w **Podręczniku bezpieczeństwa.**

12.2 ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO

Zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych obejmują m.in. wdrożone procesy zarządzania uprawnieniami i kontroli dostępu bezpieczne korzystanie i eksploatację sprzętu, zapewnienie ciągłości działania procesów związanych z przetwarzaniem danych osobowych. Szczegółowe informacje w tym zakresie opisano w **Procedurze zarządzania systemem informatycznym.**

12.3 ZABEZPIECZENIA ORGANIZACYJNE

Zabezpieczenia organizacyjne powinny być realizowane w sposób następujący:

1. AD wyznaczył IOD na drodze Zarządzenia oraz poinformował o tym fakcie pracowników, wraz ze wskazaniem danych kontaktowych IOD.
2. AD udostępnił pracownikom wdrożoną dokumentację ochrony danych osobowych, obejmującą w szczególności niniejszą **Politykę** oraz **Podręcznik bezpieczeństwa** i zobowiązał ich do przestrzegania jej założeń.
3. Osoby posiadające dostęp do danych osobowych powinny posiadać pisemne **Upoważnienie do przetwarzania danych osobowych wraz z oświadczeniem** o zachowaniu poufności nadane przez AD.
4. Upoważnienia wydawane są przez osobę z Działu Członkowsko-Organizacyjnego lub osobę pisemnie upoważnioną przez AD w oparciu o zakres wykonywanych obowiązków służbowych. Odbiór upoważnienia następuje w momencie zakończenia pracy lub w ramach odrębnej decyzji AD. Fakt o odebraniu upoważnienia jest odnotowywany w **Ewidencji osób upoważnionych** do przetwarzania danych osobowych.
5. AD przyjmuje, że upoważnienia i oświadczenia wydane na innych formularzach lub w innej, pisemnej formie nie tracą mocy prawnej do momentu wycofania tych uprawnień przez AD, lub do momentu, gdy upoważnienia powołują się na nieaktualną podstawę prawną.
6. Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy i podpisały stosowne oświadczenie, zgodnie z ust. 4 niniejszego punktu. Dokument ten uzupełniany jest w momencie podpisywania umowy o pracę, staż, praktykę, zlecenie, o dzieło lub inną formę współpracy. Za wydanie dokumentu odpowiedzialna jest osoba przygotowująca umowę z tą osobą.

1) AD prowadzi **Ewidencję osób upoważnionych do przetwarzania danych osobowych**.
2) Osoby zatrudnione lub wykonujące pracę na rzecz Spółdzielni, przy przetwarzaniu danych zostały zaznajomione z wewnętrznymi przepisami dotyczącymi ochrony danych osobowych obowiązujących w Spółdzielni m.in. poprzez zapoznanie się z niniejszym dokumentem oraz z **Podręcznikiem bezpieczeństwa,** co osoba poświadcza podpisem.

7. Osoby zatrudnione przy przetwarzaniu danych osobowych zostały przeszkolone w zakresie zabezpieczeń systemu informatycznego, z uwzględnieniem zagrożeń informatycznych i zasad postępowania, gdzie za przeszkolenie w zakresie pracy w systemie informatycznym odpowiada ASI.

12.4 ZASADY BEZPIECZEŃSTWA W RELACJACH Z KONTRAHENTAMI

W ramach prowadzonych procesów w Spółdzielni dokonuje się również zlecania określonych usług kontrahentom zgodnie z warunkami danej umowy. Wyznaczona osoba z danego działu / jednostki dokonuje bezpośredniego nadzoru nad usługami realizowanymi przez kontrahentów, w szczególności w przypadku udostępniania stronom określonych dokumentów bądź danych.

W ramach sprawowania nadzoru nad stroną zewnętrzną, uwzględnia się:

- sposób prowadzenia nadzoru i jego skuteczność (tj. realizacja postanowień umowy);
- dostęp kontrahenta do określonych zasobów Spółdzielni (np. przekazywanie niezbędnych dokumentów do rozliczenia, powierzenie przetwarzania danych osobowych, zasady dostępu do danych osobowych osób posiadających tytuł prawny do lokalu),

- potencjalny wpływ dostarczanych z zewnątrz usług na realizację głównych procesów Spółdzielni oraz zapewnienie zgodności z wymaganiami prawnymi i wewnętrznymi.

W zakresie zlecenia kontrahentom realizacji określonych usług sporządzane są umowy lub zapisy dotyczące zachowania tajemnicy, a w przypadku przekazywania danych osobowych – umowy powierzenia lub także zapisy dotyczące udostępnienia określonych danych. W zakresie umów o współpracy mogą być ustalane wymagania dotyczące m.in. dostępu dostawcy do środków przetwarzania informacji Spółdzielni, obowiązki w zakresie ochrony informacji, w tym danych osobowych, zgłaszania naruszeń w zależności od warunków określonych w umowie. W przypadku zmian w świadczeniu usług przez dostawcę są one odnotowywane w umowie o współpracy (np. poprzez aneks).

13 ZARZĄDZANIE NARUSZENIAMI OCHRONY DANYCH OSOBOWYCH

13.1 POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Instrukcja definiuje katalog zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych oraz sposób reagowania. Celem instrukcji jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa, ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości. W instrukcji przyjęto następujące zasady:

1. Każdy pracownik Spółdzielni, w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest poinformować o tym fakcie bezpośredniego przełożonego oraz IOD. Dopuszcza się również sytuację, gdy w imieniu osoby zgłaszającej poinformowania IOD dokonuje bezpośredni przełożony lub kierownik działu.
2. Punktem kontaktowym w związku z naruszeniem ochrony danych osobowych jest IOD.
3. Do typowych zagrożeń bezpieczeństwa danych osobowych, które mogą powodować naruszenie ochrony danych osobowych i podlegają zgłoszeniu należą m.in.:
    - niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;
    - niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych;
    - nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek);
    - zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności);
    - zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych);
    - umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania);
    - zgubienie lub kradzież nośników danych (laptopów, smartfonów) bez względu, czy nośnik był zaszyfrowany;
    - zgubienie, kradzież lub błędne przekazanie informacji zawierających dane osobowe (np. do niewłaściwego odbiorcy – w formie papierowej, elektronicznej);
    - pozostawienia w niezabezpieczonej lokalizacji dokumentacji papierowej z danymi osobowymi;
    - utraty przez operatora pocztowego korespondencji papierowej;
    - otrzymanie otwartej lub uszkodzonej korespondencji papierowej od operatora pocztowego;
    - nieuprawnionego uzyskania dostępu do informacji;
    - nieuprawnionego uzyskania dostępu do informacji przez złamanie zabezpieczeń (zarówno fizycznych jak i teleinformatycznych);
    - uzyskania przez pozornie zaufaną osobę poufnych informacji organizacji w oficjalnej komunikacji ustnej i pisemnej, również w formie elektronicznej;
    - nieprawidłowej anonimizacji danych osobowych w dokumentach;

- nieprawidłowego usunięcia lub zniszczenia danych osobowych z nośnika/urządzenia elektronicznego przed jego zbyciem;
- niezamierzonej publikacji;
- przesłania korespondencji w formie standardowej i elektronicznej do niewłaściwego odbiorcy;
- ujawnienia danych niewłaściwej osobie;
- ustnego ujawnienia danych.

4. IOD informowany jest niezwłocznie od momentu wykrycia naruszenia, lecz nie później niż w terminie 12 godzin.
5. Przy zgłoszeniu do IOD zagrożenia lub naruszenia należy wypełnić **Raport z incydentu** i przekazać go IOD (np. w formie skanu dokumentu). Do raportu należy dołączyć dowody stwierdzające zagrożenie lub incydent, np.:
   - korespondencję mailową;
   - zdjęcie;
   - kopię lub odpis notatki;
   - wyciąg z systemu informatycznego (jeśli to jego dotyczy naruszenie).
6. W przypadku stwierdzenia wystąpienia zagrożenia lub naruszenia ochrony danych osobowych i zgłoszenia go do IOD. IOD prowadzi postępowanie wyjaśniające, w toku, którego:
   - wspiera AD przy ustaleniu zakresu i przyczyny zagrożenia oraz ustalenia jego ewentualnych skutki dla ochrony danych osobowych Spółdzielni i osób, których te dane dotyczą;
   - inicjuje ewentualne działania dyscyplinarne oraz działania korygujące poprzez wydawanie zaleceń w związku z zidentyfikowanym zagrożeniem;
   - może zarekomendować AD działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości;
   - odnotowuje prowadzone postępowania w **Rejestrze incydentów**.
7. IOD może przekazać do AD informacje o uzupełnieniu informacji o naruszeniu i konsultuje z nim konsekwencje naruszenia dla osoby, której dane dotyczą.
8. W zakresie oceny wagi naruszenia pod kątem ryzyka naruszenia praw i wolności osób, których dane dotyczą. IOD przeprowadza ocenę w **Rejestrze incydentów** i informuje o wynikach tej oceny AD.
9. W przypadku, gdy doszło do naruszenia ochrony danych osobowych oraz to naruszenie powoduje wysokie ryzyko naruszenia praw lub wolności osób, AD zobowiązany jest zgłosić taki fakt do Prezesa Urzędu Ochrony Danych Osobowych (PUODO) w terminie 72 h od powzięcia informacji o naruszeniu, zgodnie z art. 33 ust. 1 RODO, chyba, że jest mało prawdopodobne, aby naruszenie skutkowało ryzykiem naruszenia praw i wolności osób. Decyzję w tym zakresie podejmuje AD w konsultacji z IOD w terminie 24h od powzięcia informacji o naruszeniu.
10. W przypadku, gdy naruszenie powoduje wysokie ryzyko naruszenia praw lub wolności osób, AD zgłasza ten fakt PUODO w terminie 72h od powzięcia informacji o naruszeniu, zgodnie z instrukcjami dostępnymi na stronie PUODO pod adresem: https://uodo.gov.pl/pl/p/dla-administratora. Zgłoszenie naruszenia do PUODO AD konsultuje z IOD.
11. AD zobowiązany jest do dokumentowania wszelkich naruszeń ochrony danych osobowych oraz okoliczności naruszenia danych osobowych, skutków tego naruszenia i podjętych działań naprawczych.
12. Podmioty, którym AD powierzył przetwarzanie danych są zobowiązane poprzez odpowiednie klauzule w umowach do zgłoszenia naruszenia powierzonych danych, do którego doszło u tych podmiotów – w terminie 24 h lub w terminie wskazanym w odrębnych umowach powierzenia.

13.2 ZAWIADAMIANIE OSÓB, KTÓRYCH DANE DOTYCZĄ, O NARUSZENIU

Jeżeli zidentyfikowane naruszenie ochrony danych osobowych powoduje wysokie ryzyko naruszenia praw i wolności osób, AD zobowiązany jest do niezwłocznego poinformowania osób, których dane zostały naruszone, o tym naruszeniu. Do form zawiadomienia osoby, której dane dotyczą można wykorzystać następujące kanały komunikacyjne:

- Adres e-mail osoby;
- Adres zamieszkania / korespondencyjny osoby;
- Osobiste przekazanie zawiadomienia w formie rozmowy zakończonej notatką służbową;
- Publiczny komunikat na stronie internetowej w sytuacji, gdy nie jest możliwe bezpośrednie zawiadomienie osoby.

Zawiadomienie do osoby dotyczące naruszenia ochrony danych osobowych zawiera w szczególności:

- Opis charakteru naruszenia, w tym kategorie danych osobowych, które zostały naruszone;
- Opis możliwych konsekwencji naruszenia ochrony danych osobowych i zalecenia dla osoby;
- Opis zastosowanych lub planowanych do zastosowania przez AD środków w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków dla osoby;
- Dane kontaktowe Inspektora Ochrony Danych lub inny punkt kontaktowy, od którego osoba może uzyskać więcej informacji w związku z naruszeniem;
- Jeżeli dotyczy – informację o zgłoszeniu naruszenia do Prezesa Urzędu Ochrony Danych Osobowych lub innego organu nadzorczego właściwego na miejsce przetwarzania danych.

Zawiadomienie osób, których dane dotyczą konsultowane jest z IOD i przekazywane osobom przez AD w ustalonej formie. Zawiadomienie do osoby podpisywane jest przez AD (przez Zarząd lub bezpośrednio przez Prezesa Zarządu).

AD podejmuje decyzję o zawiadomieniu osób o naruszeniu po uwzględnieniu wdrożonych środków technicznych i organizacyjnych ochrony danych, m.in. szyfrowania uniemożliwiającego odczyt osobom nieuprawnionym do dostępu do tych danych osobowych, eliminujących prawdopodobieństwo wysokiego ryzyka.

Jeżeli AD podejmie decyzję, że zastosowane środki są wystarczające lub nie, pisemnie zawiadamia IOD o każdej z tych decyzji.

14 ZASADY WSPÓŁPRACY Z ORGANEM NADZORCZYM

14.1 ZAWIADOMIENIA KIEROWANE DO ORGANU NADZORCZEGO

AD, reprezentowany przez Zarząd lub osoby przez niego wyznaczone, zobowiązany jest do niezwłocznego, lecz nie później niż w terminie 14 dni od dnia powzięcia decyzji, zawiadomienia organu w sprawach w szczególności dotyczących:

- Wyznaczenia Inspektora Ochrony Danych, zmiany jego danych kontaktowych lub jego odwołania;
- Wyznaczenia Zastępcy Inspektora Ochrony Danych, zmiany jego danych kontaktowych lub jego odwołania – jeżeli Administrator podjął decyzję o jego wyznaczeniu;
- Zmianie danych Administratora.

Zawiadomienia realizowane są drogą elektroniczną w sposób określony na stronie internetowej organu nadzorczego.

14.2 WSPÓŁPRACA Z ORGANEM NADZORCZYM W ZWIĄZKU Z NARUSZENIEM OCHRONY DANYCH OSOBOWYCH

AD dokonuje zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu w przypadku, gdy naruszenie to z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą. Zgłoszenie naruszenia do PUODO dokonywane jest w terminie 72h po stwierdzeniu naruszenia.

Zgłoszenia do PUODO można dokonać:

- Elektronicznie poprzez wypełnienie dedykowanego formularza elektronicznego dostępnego bezpośrednio na platformie biznes.gov.pl będącego odwzorowaniem formularza dostępnego na stronie PUODO;
- Elektronicznie poprzez wysłanie wypełnionego formularza na elektroniczną skrzynkę podawczą ePUAP: /UODO/SkrytkaESP;
- Elektronicznie poprzez wysłanie wypełnionego formularza zgłoszenia naruszenia ochrony danych osobowych opublikowanego na stronie internetowej organu nadzorczego, za pomocą pisma ogólnego dostępnego na platformie biznes.gov.pl;
- Tradycyjną pocztą wysyłając wypełniony formularz zgłoszenia naruszenia ochrony danych osobowych opublikowany na stronie organu, na adres organu.

Jeżeli naruszenie dotyczy danych osób w różnych krajach UE, PUODO może być, ale nie musi być wiodącym (czyli właściwym dla administratora lub podmiotu przetwarzającego) organem nadzorczym. W przypadku transgranicznego naruszenia danych administrator dokonuje analizy, czy wiodącym organem nadzorczym w odniesieniu do czynności przetwarzania, które zostały objęte naruszeniem jest PUODO, czy też może inny europejski organ nadzorczy.

W zakresie, gdy organem właściwym jest PUODO stosuje się postępowanie określone powyżej. W przypadku, gdy do 72h AD nie zgromadził całości dokumentacji w związku z naruszeniem, dokonuje zgłoszenia wstępnego.

W zgłoszeniu do PUODO AD zawiera informacje dotyczące:

a) charakteru naruszenia, w tym wskazuje w miarę możliwości kategorie i przybliżoną liczbę osób, których dane dotyczą, kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
b) imię, nazwisko, dane kontaktowe IOD lub dane kontaktowe innego punktu, od którego PUODO może uzyskać więcej informacji w związku z naruszeniem;
c) możliwych konsekwencji naruszenia ochrony danych osobowych;
d) zastosowane lub proponowane środki w celu zaradzenia naruszeniu ochrony danych osobowych oraz w stosownych przypadkach, środki w celu zminimalizowania ewentualnych negatywnych skutków naruszenia;
e) zgromadzonych dowodów w związku z naruszeniem – informacje te mogą zostać udostępnione na pisemne żądanie organu.

Zgłoszenie naruszenia ochrony danych osobowych do PUODO AD uprzednio konsultuje z IOD.

15 OCENA RYZYKA I OCENA SKUTKÓW DLA DANYCH OSOBOWYCH

Ocena i analiza ryzyka dla przetwarzanych danych osobowych przeprowadzana jest zgodnie z zasadami opisanymi w poniższej **Procedurze oceny ryzyka**.

15.1 ANALIZA RYZYKA

Spółdzielnia analizuje ryzyko utraty integralności, dostępności lub poufności informacji chronionych poprzez zestawienie możliwych zagrożeń i skutków ich zmaterializowania się - z prawdopodobieństwem ich zaistnienia.

Analiza jest wykonywana przez Zespół ds. analizy ryzyka, w skład którego wchodzą osoby wyznaczone przez Administratora.

Analizy dokonuje się w następujący sposób:

1. Na **arkuszu analizy ryzyka** zdefiniowane są możliwe zagrożenia dla bezpieczeństwa informacji. Zespół ds. analizy ryzyka może rozszerzać listę o dodatkowe zagrożenia mające wpływ na bezpieczeństwo informacji chronionych.
2. Należy określić prawdopodobieństwo wystąpienia zagrożenia, czyli przewidywanej częstotliwości występowania zagrożenia w danym obszarze / w ramach danego aktywu, zgodnie z poniższą skalą (biorąc pod uwagę całość działalności Spółki należy wskazać najwyższą przewidywaną wartość):

Wartość	Prawdopodobieństwo	Uwagi

1	Bardzo niskie / Incydentalne	Dotychczas nie zidentyfikowano wystąpienia zagrożenia, zdarzenie może się urealnić w pewnych wyjątkowych okoliczności, przy wystąpieniu ściśle określonych czynników i zakłada się, że zdarzenie mogące mieć wpływ na wystąpienie zagrożenia będzie miało charakter incydentalny, pojedynczego zdarzenia w całej organizacji, lecz praktycznie nie występuje w organizacji.
2	Rzadkie	Zakłada się, że zagrożenia mogą występować rzadko. Istnieją zapisy lub dowody na wystąpienie zdarzenia w przeszłości, w szczególności w ramach pojedynczego zdarzenia w danym referacie / komórce organizacji i kilkukrotnie w ciągu roku w całej organizacji.
3	Znaczne	Zakłada się ze zagrożenia mogą się urealnić I wystąpić niezależnie od panujących okoliczności w organizacji. Mogą występować okoliczności zwiększające prawdopodobieństwo wystąpienia konkretnego zdarzenia. Dotychczas zidentyfikowano kilkukrotne wystąpienie zagrożenia w danych referatach / komórkach organizacyjnych w organizacji w ciągu roku.
4	Bardzo wysokie	Oczekuje się, że zagrożenia wystąpią w większości przypadków lub okoliczności. Dotychczas zidentyfikowano wielokrotne wystąpienie zdarzeń mających wpływ na wystąpienia zagrożenia w organizacji, zdarzenia wielokrotnie identyfikowano w referatach / komórkach organizacji. Istnieją dowody potwierdzające wystąpienie zagrożeń w przeszłości oraz zmaterializowania się skutków oraz przyczyn.

3. Należy wskazać możliwe konsekwencje zmaterializowania się zagrożenia w odniesieniu do potencjalnych strat dla Spółki zgodnie z poniższą skalą (biorąc pod uwagę całość działalności Urzędu należy wskazać najwyższą przewidywaną wartość):

Wartość skutku	Uwagi
1	Zagrożenie nie spowoduje negatywnych konsekwencji.
2	Zagrożenie może spowodować przejściowe niedogodności.
3	Zagrożenie spowoduje straty wizerunkowe, finansowe.
4	Zagrożenie spowoduje znaczne straty oraz może powodować narażenie zdrowia i życia osób.

4. Należy określić wartość ryzyka według poniższego wzoru:

$$R = P \times S$$

gdzie:

R – wartość ryzyka (w arkuszu definiowany jako: Ryzyko).

P – prawdopodobieństwo wystąpienia danego zdarzenia,

S – oznacza skutek, czyli konsekwencje całkowite zmaterializowania się danego zagrożenia w odniesieniu do organizacji i osób, których dane dotyczą, przy czym prawdopodobieństwo wystąpienia konkretnego zagrożenia zawsze odpowiada jednemu konkretnemu skutkowi.

Poziom ryzyka wyliczany jest automatycznie na arkuszu i jest klasyfikowany jako:

Poziom ryzyka		Zakres
Minimalne		1 - 2
Małe		3 - 4

Średnie		6 - 8
Wysokie		12-16

5. Należy podjąć decyzję co do reakcji na ryzyko. Kryteria akceptacji ryzyka znajdują się w poniższej tabeli:

Poziom ryzyka		Postępowanie	Zakres	Uwagi
Minimalne		Akceptacja	1 - 2	Nie wymaga działania
Małe		Akceptacja/Postępowanie	3 - 4	Może wymagać redukcji ryzyka
Średnie		Postępowanie	6 - 8	Wymagana redukcja ryzyka
Wysokie		Unikanie	12-16	Należy rozważyć unikanie ryzyka

W przypadku poziomu ryzyka, który wymaga reakcji Zespół ds. analizy ryzyka proponuje sposób redukcji ryzyka. Wybrany sposób postępowania z ryzykiem należy udokumentować na **Arkuszu analizy ryzyka** wraz z określeniem planowanego terminu wdrożenia działań.

Proces oceny ryzyka jest przeprowadzany co najmniej raz w roku, aby upewnić się, czy:

- Ryzyko nadal występuje?
- Pojawiło się nowe ryzyko?
- Prawdopodobieństwo i następstwa ryzyka zmieniły się?
- Stosowane środki kontroli są skuteczne?

Zespół ds. analizy ryzyka przeprowadza coroczne szacowanie ryzyka na podstawie informacji otrzymanych od pracowników oraz wyników poprzednich analiz. W przypadku wykonywania drugiej i kolejnych corocznych analiz ryzyka należy się w nich odnieść do stopnia realizacji zatwierdzonych działań w reakcji na podwyższone ryzyko. Wyniki oceny ryzyka są przedstawiane do zatwierdzenia Zarządowi, który podejmuje decyzję, co do ewentualnej realizacji zaproponowanych działań. Analiza ryzyka powinna też zostać wykonana w sytuacji zmian w Spółdzielni, które mogą mieć wpływ na bezpieczeństwo danych – takich jak wdrożenie nowego systemu teleinformatycznego itp. Analizę tą można wykonać za pośrednictwem **Arkusza analizy ryzyka nowego procesu.**

16 ODPOWIEDZIALNOŚĆ PRACOWNIKÓW

Podczas przetwarzania danych osobowych, użytkownicy są zobowiązani do stosowania postanowień zawartych w niniejszej **Polityce** oraz innych dokumentach dotyczących ochrony danych osobowych oraz bezpieczeństwa informacji przyjętych u AD. Pracownicy ponoszą pełną odpowiedzialność za ochronę powierzonych im danych osobowych. Zasady oraz odpowiedzialność pracowników oraz członków organów statutowych za przetwarzane dane opisano w **Podręczniku bezpieczeństwa**.

17 POSTANOWIENIA KOŃCOWE

W sprawach nieuregulowanych w niniejszej **Polityce** mają zastosowanie obowiązujące przepisy o ochronie danych osobowych, w szczególności RODO. Niniejsza **Polityka** podlega przeglądowi co najmniej raz w roku pod kątem jej aktualności.

Niniejsza **Polityka Bezpieczeństwa Danych Osobowych** wchodzi w życie na podstawie uchwały Rady Nadzorczej nr …….. Jednocześnie traci moc Regulamin Ochrony Danych Osobowych przyjęty uchwałą RN nr 16/2018 z dnia 28 sierpnia 2018 r.

18 ZAŁĄCZNIKI

1. Załącznik nr 1 – Podręcznik bezpieczeństwa;
2. Załącznik nr 2 – Instrukcja Zarządzania Systemem Teleinformatycznym;
3. Załącznik nr 3 – Rejestr czynności przetwarzania;
4. Załącznik nr 3B – Rejestr kategorii czynności przetwarzania;
5. Załącznik nr 4 – Wniosek o nadanie / zmianę / cofnięcie uprawnień w systemie informatycznym;

6. Załącznik nr 5, 5A, 5B, 5C, 5D, 5E, 5F, 5G – Upoważnienie do przetwarzania danych osobowych wraz z oświadczeniami;
7. Załącznik nr 6 – Rejestr osób upoważnionych do przetwarzania danych osobowych;
8. Załącznik nr 7 – Raport z incydentu;
9. Załącznik nr 8 – Rejestr incydentów;
10. Załącznik nr 8B – Waga naruszenia;
11. Załącznik nr 9 – Ewidencja zagrożeń;
12. Załącznik nr 10 – Kwestionariusz oceny podmiotu;
13. Załącznik nr 11 – Zgłoszenie realizacji praw z zakresu Danych Osobowych;
14. Załącznik nr 12 – Prezentacja szkoleniowa z zakresu Ochrony Danych Osobowych;
15. Załącznik nr 13 – Test równowagi;
16. Załącznik nr 14 – Arkusz analizy ryzyka;
17. Załącznik nr 15 – Arkusz analizy ryzyka nowego procesu;
18. Załącznik nr 16 – Oświadczenie o zachowaniu poufności