

REGULAMIN OCHRONY DANYCH OSOBOWYCH

Czeladzka Spółdzielnia Mieszkaniowa w Czeladzi

SPIS TREŚCI

A. INFORMACJE OGÓLNE	3
1. Cel Polityki ochrony danych osobowych	3
2. Terminologia.....	4
3. Zakres informacji objętych Polityką ochrony danych osobowych oraz zakres zastosowania	6
B. OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH	7
1. Struktura organizacji ochrony danych osobowych	7
1.1. Administrator Danych.....	7
1.2. Inspektor Ochrony Danych	9
1.3. Administrator Systemów Informatycznych.....	10
1.4. Osoby upoważnione do przetwarzania danych osobowych	11
C. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH	12
1. Ogólne zasady przetwarzania danych osobowych	12
2. Zakres przetwarzanych danych osobowych.....	13
3. Dopuszczenie osób do przetwarzania danych osobowych.....	15
4. Powierzenie przetwarzania danych osobowych.....	16
5. Udostępnienie danych osobowych	18
6. Przekazywanie danych osobowych do państw trzecich.....	19
7. Współadministrowanie danymi osobowymi	21
8. Audyty zgodności przetwarzania danych osobowych	22
9. Realizacja praw osób, których dane dotyczą	23
10. Ochrona danych osobowych w fazie projektowania oraz domyślna ochrona danych osobowych	24
11. Ocena skutków dla ochrony danych osobowych (<i>data protection impact assessment</i>).....	25
12. Incydenty ochrony danych osobowych	26
13. Ogólne zasady bezpieczeństwa ochrony danych osobowych	27
14. Przeglądy i aktualizacja Polityki ochrony danych osobowych.....	29
15. Załączniki.....	30

A. INFORMACJE OGÓLNE

1. CEL POLITYKI OCHRONY DANYCH OSOBOWYCH

Regulamin ochrony danych osobowych zostały opracowany i wdrożony w strukturze Administratora Danych w celu zapewnienia zgodności przetwarzania danych osobowych z wymogami obowiązujących w tym zakresie polskich i europejskich aktów prawnych, w szczególności:

1. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),
2. Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2018 r., poz. 1000 ze zm.).

Regulamin ochrony danych osobowych ma zastosowanie do wszystkich pracowników Administratora Danych, którzy w zakresie swoich obowiązków służbowych przetwarzają dane osobowe, jak również innych osób, które z upoważnienia Administratora Danych uzyskały dostęp do danych osobowych. Każda z tych osób została zapoznana z najważniejszymi procedurami bezpieczeństwa danych opisanymi w Polityce ochrony danych osobowych i zobowiązana do ich przestrzegania w zakresie wynikającym z przydzielonych zadań. Osoby, o których mowa złożyły oświadczenie o zapoznaniu się z procedurami bezpieczeństwa danych oraz zobowiązały się do ich stosowania.

Wszelkie wątpliwości dotyczące sposobu interpretacji zapisów Polityki ochrony danych osobowych, powinny być rozstrzygane na korzyść zapewnienia możliwie najwyższego poziomu ochrony danych osobowych oraz realizacji praw osób, których dane dotyczą.

2. TERMINOLOGIA

1. **Administrator Danych (ADO)** – Czeladzka Spółdzielnia Mieszkaniowa w Czeladzi,
2. **Administrator Systemów Informatycznych (ASI)** – osoba wyznaczona przez Administratora Danych, koordynująca działania związane z zapewnieniem bezpieczeństwa systemów informatycznych, w tym również odpowiadająca za nadzór nad zabezpieczeniem danych osobowych przetwarzanych w systemach informatycznych wykorzystywanych przez Administratora Danych,
3. **dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”), gdzie poprzez możliwą do zidentyfikowania osobę fizyczną rozumie się osobę, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej,
4. **DPIA** – ocena skutków dla ochrony danych osobowych (*data protection impact assessment*),
5. **Inspektor Ochrony Danych (IOD)** – osoba wyznaczona przez Administratora Danych, koordynująca procesy związane z przestrzeganiem zasad ochrony danych osobowych w ramach procesów przetwarzania danych osobowych zachodzących w strukturze Administratora Danych,
6. **organ nadzorczy** – niezależny organ publiczny w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych osobowych w Unii, powołany w każdym państwie członkowskim Unii, którego podstawowym zadaniem jest monitorowanie stosowania RODO,
7. **państwo trzecie** – państwo nienależące do Europejskiego Obszaru Gospodarczego.
8. **podmiot przetwarzający** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora Danych,
9. **regulamin** – niniejszy regulamin ochrony danych osobowych,
10. **pracownik** – osoba współpracująca z Administratorem Danych na podstawie umowy o pracę lub umowy cywilnoprawnej,
11. **przetwarzanie** – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką 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,

12. **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 (ogólne rozporządzenie o ochronie danych),
13. **Unia** – Unia Europejska,
14. **Ustawa** – Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2018 r., poz. 1000 ze zm.),

3. ZAKRES INFORMACJI OBJĘTYCH POLITYKĄ OCHRONY DANYCH OSOBOWYCH ORAZ ZAKRES ZASTOSOWANIA

Regulamin ochrony danych osobowych opisuje zasady i procedury przetwarzania danych osobowych. Jest to zestaw praw, reguł i praktycznych doświadczeń dotyczących sposobu zarządzania, ochrony i dystrybucji danych osobowych wewnątrz Administratora Danych. Regulamin odnosi się całościowo do problemu zabezpieczenia danych osobowych, tj. zarówno do zabezpieczenia danych przetwarzanych tradycyjnie, jak i danych przetwarzanych w systemach informatycznych.

Politykę ochrony danych osobowych stosuje się do wszelkich czynności, stanowiących w myśl RODO, przetwarzanie danych osobowych. Bez względu na źródło pochodzenia danych osobowych, ich zakres, cel zebrania, sposób przetwarzania lub czas przetwarzania, stosowane są zasady ujęte w Regulaminie.

Rygorowi Regulaminu podlegają także dane powierzone Administratorowi Danych do przetwarzania na podstawie umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego oraz dane osobowe, które zostały Administratorowi Danych udostępnione.

B. OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH

1. STRUKTURA ORGANIZACJI OCHRONY DANYCH OSOBOWYCH

Za przetwarzanie danych osobowych oraz ich ochronę zgodnie z postanowieniami RODO, Ustawy, Polityki oraz procedur wewnętrznych z zakresu ochrony danych osobowych wdrożonych w strukturze Administratora Danych, odpowiadają:

1. Administrator Danych,
2. Inspektor Ochrony Danych,
3. Administrator Systemów Informatycznych,
4. Osoby upoważnione do przetwarzania danych osobowych.

1.1. ADMINISTRATOR DANYCH

1. Administrator Danych wyznacza:
 - 1.1. IOD,
 - 1.2. Administratora Systemów Informatycznych.
2. Administrator Danych jest odpowiedzialny za:
 - 2.1. zapewnienie odpowiednich środków organizacyjnych i technicznych w celu zapewnienia i wykazania przetwarzania danych osobowych zgodnie z określonymi w RODO zasadami przetwarzania danych osobowych,
 - 2.2. wdrożenie odpowiednich procedur ochrony danych osobowych,
 - 2.3. jeśli uzna to za konieczne, stosowanie zatwierdzonych kodeksów postępowania lub zatwierdzonych mechanizmów certyfikacji, jako element dla stwierdzenia przestrzegania przez Administratora Danych ciężących na nim obowiązków,
 - 2.4. zapewnienie środków umożliwiających prawidłową realizację praw osób, których dane dotyczą,
 - 2.5. prowadzenie rejestru czynności przetwarzania danych osobowych,
 - 2.6. prowadzenie rejestru kategorii przetwarzania dokonywanych w imieniu innego administratora,
 - 2.7. współpracę z organem nadzorczym w ramach wykonywania przez niego swoich zadań,

- 2.8. wdrożenie odpowiednich środków organizacyjnych i technicznych, aby zapewnić stopień bezpieczeństwa odpowiadający istniejącemu ryzyku naruszenia praw lub wolności osób, których dane dotyczą,
- 2.9. zgłaszanie naruszenia ochrony danych osobowych właściwemu organowi nadzorcemu, a w przypadku, gdy zajądą ku temu odpowiednie przesłanki, również osobie, której dane dotyczą,
- 2.10. dokumentowanie wszelkich naruszeń ochrony danych osobowych, w tym okoliczności naruszenia, jego skutków oraz podjętych działań zaradczych,
- 2.11. zapewnienie odpowiednich środków w celu dokonania oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych w sytuacji, jeżeli dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, w tym, jeżeli zajądą ku temu odpowiednie przesłanki, konsultację z organem nadzorczym,
- 2.12. nadawanie upoważnień do przetwarzania danych osobowych oraz prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
- 2.13. zapewnienie legalności przekazywania danych osobowych do podmiotów trzecich,
- 2.14. w stosunku do IOD:
 - 2.14.1. zapewnienie, że jest on właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych,
 - 2.14.2. wspieranie IOD w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej,
 - 2.14.3. zagwarantowanie by IOD nie działał pod wpływem presji i nie otrzymywał instrukcji dotyczących wykonywania swoich zadań,
 - 2.14.4. publikację danych kontaktowych IOD oraz zawiadomienie o nich organu nadzorczego.
3. Administrator Danych nadzoruje działania IOD oraz ASI oraz wydaje im zalecenia, co do sposobu wykonywania obowiązków wynikających z Polityki.
4. Administrator Danych każdorazowo wyraża zgodę oraz ostateczną akceptację na kluczowe z perspektywy organizacji działania IOD oraz ASI, w które zaangażowane są podmioty trzecie. Do zaakceptowania tych działań, wystarczająca jest zgoda wyrażona w formie wiadomości e-mail.

1.2. INSPEKTOR OCHRONY DANYCH

1. Funkcję IOD pełni osoba wyznaczona przez Administratora Danych.
2. IOD jest wyznaczany przez Administratora Danych na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia swoich zadań.
4. Do zadań IOD należy:
 - 4.1. informowanie o obowiązkach wynikających z RODO oraz innych właściwych przepisów Unii lub państw członkowskich o ochronie danych osobowych oraz doradzanie w tym zakresie,
 - 4.2. monitorowanie przestrzegania RODO oraz innych właściwych przepisów Unii lub państw członkowskich o ochronie danych osobowych,
 - 4.3. monitorowanie przestrzegania wdrożonych procedur ochrony danych osobowych,
 - 4.4. doradztwo w zakresie podziału obowiązków (np. między współadministratorami, Administratorem Danych a podmiotem przetwarzającym lub pomiędzy pracownikami Administratora Danych),
 - 4.5. działania zwiększające świadomość pracowników Administratora Danych w zakresie obowiązków wynikających z RODO lub przyjętych procedur,
 - 4.6. szkolenia dla pracowników Administratora Danych uczestniczących w operacjach przetwarzania danych,
 - 4.7. przeprowadzanie audytów w zakresie przestrzegania RODO i wdrożonych procedur ochrony danych osobowych,
 - 4.8. udzielanie na żądanie zaleceń, co do oceny skutków dla ochrony danych osobowych oraz monitorowanie jej wykonania,
 - 4.9. współpraca z organem nadzorczym oraz pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych,
 - 4.10. pełnienie funkcji punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO.

1.3. ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH

1. Funkcję ASI pełni osoba wyznaczona przez Administratora Danych.
2. Do zadań ASI należy:
 - 3.1. prowadzenie rejestru nadanych uprawnień do systemów informatycznych,
 - 3.2. nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów,
 - 3.3. podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń,
 - 3.4. identyfikacja i analiza zagrożeń oraz ocena ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych,
 - 3.5. sprawowanie nadzoru nad kopiami zapasowymi;
 - 3.6. inicjowanie i nadzór nad wdrażaniem nowych narzędzi, procedur organizacyjnych oraz sposobów zarządzania systemami informatycznymi, które mają doprowadzić do wzmocnienia bezpieczeństwa przy przetwarzaniu danych osobowych,
 - 3.7. podejmowanie innych czynności w zakresie zabezpieczenia przetwarzania danych w systemach informatycznych,
 - 3.8. dokonywanie cyklicznych przeglądów aktualności i stosowania procedur z zakresu przetwarzania danych w systemach informatycznych, na podstawie opracowanego planu przeglądów.
 - 3.9. ścisła współpraca z IOD w zakresie bezpieczeństwa i zasad przetwarzania danych osobowych w systemach informatycznych.

1.4. OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Każda osoba, która uzyskała upoważnienie do przetwarzania danych, zobowiązana jest do ich ochrony w sposób zgodny z przepisami RODO, Ustawy oraz postanowieniami Regulaminu.
2. Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia. Stosowny zapis o przyjęciu zobowiązania do zachowania w tajemnicy przetwarzanych danych osobowych zawiera upoważnienie, którego wzór znajduje się w Załączniku nr 1 do Regulaminu.
3. Naruszenie obowiązku ochrony danych osobowych, a w szczególności obowiązku zachowania danych osobowych w tajemnicy skutkuje poniesieniem odpowiedzialności karnej na podstawie przepisów Ustawy oraz stanowi ciężkie naruszenie obowiązków pracowniczych i może być podstawą rozwiązania stosunku pracy w trybie art. 52 Ustawy z dnia 26 czerwca 1974 r. Kodeks Pracy (tekst jedn. Dz.U. z 2018 r., poz. 108 ze zm.), bądź rozwiązania stosunku cywilnoprawnego.

C. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

1. OGÓLNE ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

1. Przetwarzanie danych osobowych w strukturze Administratora Danych odbywa się zgodnie z ogólnymi zasadami przetwarzania danych osobowych określonymi w art. 5 RODO. Oznacza to, że dane osobowe przetwarzają się:
 - 1.1 zgodnie z prawem, w oparciu o co najmniej jedną przesłankę legalności przetwarzania danych osobowych wskazaną w art. 6 lub 9 RODO (*zasada legalności*),
 - 1.2 w sposób rzetelny przy uwzględnieniu interesów i rozsądnych oczekiwań osób, których dane dotyczą (*zasada rzetelności*),
 - 1.3 w sposób przejrzysty dla osób, których dane dotyczą (*zasada przejrzystości*),
 - 1.4 w konkretnych, wyraźnych i prawnie uzasadnionych celach (*zasada ograniczenia celu*),
 - 1.5 w zakresie adekwatnym, stosownym oraz niezbędnym dla celów, w których są przetwarzane (*zasada minimalizacji danych*),
 - 1.6 przy uwzględnieniu ich prawidłowości i ewentualnego uaktualniania (*zasada prawidłowości*),
 - 1.7 przez okres nie dłuższy, niż jest to niezbędne dla celów, w których są przetwarzane (*zasada ograniczenia przechowywania*),
 - 1.8 w sposób zapewniający odpowiednie bezpieczeństwo (*integralność i poufność*).
2. Administrator Danych gwarantuje, że określone decyzje odnoszące się do procesów przetwarzania danych osobowych zostały przeanalizowane z punktu widzenia zgodności z ogólnymi zasadami przetwarzania danych, a przede wszystkim, że są z nimi zgodne.

2. ZAKRES PRZETWARZANYCH DANYCH OSOBOWYCH

1. Regulamin ma zastosowanie w stosunku do wszystkich danych osobowych przetwarzanych przez Administratora Danych, niezależnie od formy ich przetwarzania (elektroniczna lub papierowa) oraz tego, czy są to dane przetwarzane w zbiorach danych, w zestawach czy stanowią one pojedyncze informacje osobowe.
2. Wykaz zbiorów danych osobowych, których administratorem jest Administrator Danych oraz procesów przetwarzania zachodzących w tych zbiorach stanowi Załącznik nr 3 do Regulaminu.
3. Administrator Danych prowadzi:
 - 3.1. rejestr czynności przetwarzania danych osobowych, których jest administratorem,
 - 3.2. rejestr kategorii czynności przetwarzania dokonywanych w imieniu administratorów, którzy powierzyli mu przetwarzanie danych.
4. Rejestr, o którym mowa w pkt 3.1. zawiera co najmniej następujące informacje:
 - 4.1. nazwę oraz dane kontaktowe Administratora Danych oraz wszelkich współadministratorów,
 - 4.2. gdy ma to zastosowanie imię, nazwisko lub nazwę oraz dane kontaktowe swojego przedstawiciela,
 - 4.3. imię i nazwisko oraz dane kontaktowe IOD,
 - 4.4. cele przetwarzania,
 - 4.5. opis kategorii osób, których dane dotyczą,
 - 4.6. opis kategorii danych osobowych,
 - 4.7. kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych,
 - 4.8. gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazania, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń,
 - 4.9. jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,
 - 4.10. ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.
5. Rejestr, o którym mowa w pkt 3.2. zawiera co najmniej następujące informacje:
 - 5.1. nazwę oraz dane kontaktowe Administratora Danych,
 - 5.2. imię i nazwisko lub nazwę oraz dane kontaktowe każdego administratora, w imieniu którego działa Administrator Danych,

- 5.3. gdy ma to zastosowanie, imię, nazwisko lub nazwę oraz dane kontaktowe przedstawiciela każdego administratora, w imieniu którego działa Administrator Danych,
 - 5.4. gdy ma to zastosowanie, imię i nazwisko oraz dane kontaktowe IOD każdego administratora, w imieniu którego działa Administrator Danych,
 - 5.5. kategorie przetwarzań dokonywanych w imieniu każdego z administratorów,
 - 5.6. gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazania, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń,
 - 5.7. ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.
6. IOD prowadzi rejestry, o których mowa w pkt 3 w formie elektronicznej.
 7. W przypadku zgłoszenia przez organ nadzoru żądania w tym zakresie, Administrator Danych udostępni mu prowadzone przez siebie rejestry.

3. DOPUSZCZENIE OSÓB DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator Danych realizując Regulamin, w zakresie udostępniania danych osobowych w ramach własnej (wewnętrznej) struktury, zezwala na ich przetwarzanie w systemie informatycznym lub w wersji papierowej wyłącznie osobom, które uzyskały uprzednie, stosowne upoważnienie do przetwarzania danych osobowych.
2. Upoważnienie do przetwarzania danych osobowych nadawane jest po zaznajomieniu, osoby upoważnianej z zasadami ochrony danych osobowych obowiązującymi w strukturze Administratora Danych.
3. Upoważnienie do przetwarzania danych osobowych, nadawane jest indywidualnie, z wyraźnym wskazaniem, jakie zbiory danych obejmuje swoim zakresem.
4. Administrator Danych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, której wzór stanowi Załącznik nr 2 do Regulaminu.

4. POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator Danych realizując Regulamin dopuszcza, by dane osobowe, których jest administratorem były przetwarzane poza własnymi strukturami organizacyjnymi. Może się to odbywać wyłącznie na drodze powierzenia danych, w określonym celu i zakresie, podmiotowi przetwarzającemu na mocy umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego.
2. Podstawowym warunkiem dopuszczalności powierzenia przetwarzania danych w imieniu administratora jest poddanie planowanego outsourcingu analizie, która powinna zapewnić, że wybór podmiotu przetwarzającego został uzależniony od zapewnienia wystarczających gwarancji ochrony danych.
3. Zawierana przez Administratora Danych umowa powierzenia przetwarzania danych osobowych musi być zgodna z postanowieniami art. 28 RODO, tj. w szczególności określać:
 - 3.1. przedmiot powierzenia,
 - 3.2. czas trwania powierzenia,
 - 3.3. charakter i cel przetwarzania,
 - 3.4. rodzaj powierzanych danych osobowych,
 - 3.5. kategorie osób, których dane dotyczą,
 - 3.6. warunki podpowierzenia przetwarzania danych
 - 3.7. obowiązki i prawa Administratora Danych,
 - 3.8. obowiązki podmiotu przetwarzającego.
4. Umowa powierzenia może zostać zawarta w formie pisemnej, w tym elektronicznej.
5. W przypadku, gdy elementy powierzenia przetwarzania danych wskazane w pkt 3 znajdują się już w zawartej z danym podmiotem umowie, nie ma konieczności sporządzania dodatkowej umowy powierzenia przetwarzania danych osobowych.
6. Pracownik Administratora Danych odpowiedzialny za przygotowanie umowy z podmiotem przetwarzającym, przed planowanym rozpoczęciem współpracy z podmiotem przetwarzającym, jest zobowiązany poinformować o tym IOD oraz skonsultować z nim postanowienia zawieranej umowy w zakresie powierzenia przetwarzania danych osobowych. Powierzenie przetwarzania danych może odbyć się wyłącznie na podstawie postanowień zaakceptowanych przez IOD.
7. Umowa powierzenia przetwarzania danych osobowych podpisywana jest zgodnie z zasadami reprezentacji Administratora Danych lub udzielonymi pełnomocnictwami.
8. Każdorazowe dokonanie powierzenia danych osobowych musi zostać obligatoryjnie odnotowane w rejestrze czynności przetwarzania danych osobowych.

9. Administrator Danych ma prawo kontroli podmiotów przetwarzających, którym powierzył przetwarzanie danych osobowych.
10. Administrator Danych w zakresie prowadzonej przez siebie działalności może przetwarzać również dane osobowe powierzone przez podmioty, na rzecz których świadczy usługi. Przyjęcie danych w powierzenie przez Administratora Danych musi zostać obligatoryjnie odnotowane w rejestrze kategorii czynności przetwarzania danych osobowych.

5. UDOSTĘPNIENIE DANYCH OSOBOWYCH

1. Administrator Danych realizując Politykę dopuszcza, by dane osobowe, których jest administratorem były przekazywane innym administratorom w formie udostępnienia danych.
2. Udostępnienie danych osobowych może nastąpić tylko w oparciu o co najmniej jedną przesłankę spośród wskazanych w art. 6 RODO i / lub art. 9 RODO.
3. Podmioty lub kategorie podmiotów, którym udostępnia się dane osobowe muszą zostać obligatoryjnie wskazane w rejestrze czynności przetwarzania danych osobowych.

6. PRZEKAZYWANIE DANYCH OSOBOWYCH DO PAŃSTW TRZECICH

1. Przekazywanie danych, których administratorem jest Administrator Danych do państw trzecich i organizacji międzynarodowych, może się odbywać wyłącznie po spełnieniu warunków przewidzianych w Rozdziale V RODO.
2. Przekazywanie danych do państw trzecich może mieć formę zarówno powierzenia przetwarzania danych osobowych oraz udostępnienia danych osobowych, co oznacza, że w zależności od rodzaju przekazania, należy wziąć również pod uwagę postanowienia podrozdziałów 4 i 5 Polityki.
3. Przekazanie danych osobowych, których administratorem jest Administrator Danych do państwa trzeciego może nastąpić w sytuacji, jeżeli Komisja Europejska wydała decyzję, że dane państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony. Takie przekazanie nie wymaga specjalnego zezwolenia.
4. W przypadkach braku decyzji Komisji Europejskiej, o której mowa w pkt 3, dokonanie przekazania danych osobowych do państwa trzeciego jest możliwe, gdy Administrator Danych samodzielnie zapewni odpowiednie zabezpieczenia i pod warunkiem, że będą obowiązywały egzekwowalne prawa osób, których dane dotyczą i skuteczne środki ochrony prawnej. Odpowiednie zabezpieczenia Administrator Danych może zapewnić za pomocą:
 - 4.1. prawnie wiążącego i egzekwownego instrumentu między organami lub podmiotami publicznymi,
 - 4.2. wiążących reguł korporacyjnych zatwierdzonych przez organ nadzorczy, mających zastosowanie do każdego z członków grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą,
 - 4.3. standardowych klauzul ochrony danych przyjętych lub zatwierdzonych przez Komisję Europejską,
 - 4.4. standardowych klauzul ochrony danych przyjętych przez organ nadzorczy i zatwierdzonych przez Komisję Europejską,
 - 4.5. zatwierzonego kodeksu postępowania wraz z wiążącymi i egzekwownymi zobowiązaniami administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą, lub
 - 4.6. zatwierzonego mechanizmu certyfikacji wraz z wiążącymi i egzekwownymi zobowiązaniami administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą.

5. Z zastrzeżeniem zezwolenia właściwego organu nadzorczego odpowiednie zabezpieczenia, o których mowa w pkt 4 Administrator Danych może zapewnić w szczególności za pomocą:
 - 5.1. klauzul umownych między Administratorem Danych lub podmiotem przetwarzającym a Administratorem Danych, podmiotem przetwarzającym lub odbiorcą danych osobowych w państwie trzecim lub organizacji międzynarodowej, lub
 - 5.2. postanowień uzgodnień administracyjnych między organami lub podmiotami publicznymi, w których przewidziane będą egzekwowalne i skuteczne prawa osób, których dane dotyczą.
6. W szczególnych przypadkach, dopuszcza się przekazanie danych osobowych przez Administratora Danych do państwa trzeciego pomimo braku decyzji Komisji Europejskiej, o której mowa w pkt 3 oraz zapewnienia odpowiednich zabezpieczeń, o których mowa w pkt 4 i 5. Do tych szczególnych przypadków zalicza się przekazanie danych pod warunkiem, że:
 - 6.1. osoba, której dane dotyczą, poinformowana o ewentualnym ryzyku, z którymi może się dla niej wiązać proponowane przekazanie, wyrazi na nie wyraźną zgodę,
 - 6.2. przekazanie jest niezbędne do wykonania umowy zawartej z osobą, której dane dotyczą,
 - 6.3. przekazanie jest niezbędne do zawarcia lub wykonania umowy zawartej w interesie osoby, której dane dotyczą,
 - 6.4. przekazanie jest niezbędne ze względu na ważne względy interesu publicznego,
 - 6.5. przekazanie jest niezbędne ze względu na posiadane roszczenia,
 - 6.6. przekazanie jest niezbędne do ochrony żywotnych interesów osoby, których dane dotyczą lub
 - 6.7. przekazanie nastąpi z publicznego rejestru.
7. Pracownik Administratora Danych Osobowych przygotowujący umowę z podmiotem przetwarzającym, przed planowanym przekazaniem danych do państwa trzeciego, jest zobowiązany poinformować o tym IOD oraz skonsultować z nim warunki przekazania tych danych. Przekazanie danych może odbyć się wyłącznie na podstawie warunków i postanowień zaakceptowanych przez IOD.

7. WSPÓŁADMINISTROWANIE DANYMI OSOBOWYMI

1. Administrator Danych w zakresie przetwarzanych przez siebie danych osobowych dopuszcza możliwość przyjęcia modelu współadministrowania danymi osobowymi zgodnie z art. 26 RODO.
2. Współadministrowanie danymi może zachodzić wówczas, jeżeli Administrator Danych oraz co najmniej jeden inny podmiot, wspólnie ustalają cele i sposoby przetwarzania danych osobowych. Oznacza to, że w danym procesie przetwarzania danych osobowych muszą zostać spełnione równocześnie trzy warunki, tj. Administrator Danych oraz co najmniej jeden inny podmiot muszą:
 - 2.1. być administratorami w rozumieniu art. 4 pkt 7 RODO,
 - 2.2. muszą wspólnie ustalić cele przetwarzania danych,
 - 2.3. muszą wspólnie ustalić sposoby (techniczne i organizacyjne) przetwarzania danych osobowych.
3. W przypadku spełnienia warunków, o których mowa w pkt 2 Administrator Danych oraz co najmniej jeden inny podmiot stają się współadministratorami danych w zakresie danego procesu przetwarzania danych osobowych.
4. W przypadku przyjęcia modelu współadministrowania danymi, współadministratorzy danych w drodze wspólnych uzgodnień, w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO.
5. W sytuacji, kiedy w zakresie zachodzących w strukturze Administratora Danych procesów przetwarzania danych osobowych pojawią się procesy wobec których istnieje prawdopodobieństwo zachodzenia współadministrowania danymi, pracownik Administratora Danych odpowiedzialny za współpracę z podmiotem współadministrującym informuje o tym fakcie IOD.
6. IOD dokonuje oceny, czy dany proces przetwarzania spełnia warunki współadministrowania danymi.
7. W przypadku, kiedy wynik oceny, o której mowa w pkt 6 wskazuje na współadministrowanie danymi osobowymi, IOD, przy współudziale pozostałych współadministratorów, opracowuje wspólne uzgodnienia, o których mowa w pkt 4.

8. AUDYTY ZGODNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

1. Audyty zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz procedurami wdrożonymi w strukturze Administratora Danych przeprowadzane są przez IOD.
2. IOD przeprowadza audyt zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych co najmniej raz w roku.
3. W toku audytu IOD dokonuje i dokumentuje czynności, w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz do opracowania sprawozdania.
4. Po zakończeniu audytu, IOD przygotowuje dla Administratora Danych, sprawozdanie w tym zakresie. Sprawozdanie sporządzane jest w postaci elektronicznej albo w postaci papierowej.
5. IOD przekazuje Administratorowi Danych sprawozdanie nie później niż w terminie 30 dni od zakończenia audytu.

9. REALIZACJA PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ

1. Administrator Danych uwzględnia w zachodzących w jego strukturze procesach przetwarzania danych osobowych, procedury i zasady ułatwiające osobie, której dane dotyczą, wykonywanie praw przysługujących jej na mocy przepisów RODO, w tym, w szczególności:
 - 1.1. prawo do wycofania wyrażonej zgody (art. 7 ust. 3 RODO),
 - 1.2. prawo dostępu przysługujące osobie, której dane dotyczą (art. 15 RODO),
 - 1.3. prawo do sprostowania danych (art. 16 RODO),
 - 1.4. prawo do usunięcia danych (*prawo do bycia zapomnianym*) (art. 17 RODO),
 - 1.5. prawo do ograniczenia przetwarzania (art. 18 RODO),
 - 1.6. prawo do przenoszenia danych (art. 20 RODO),
 - 1.7. prawo sprzeciwu (art. 21 RODO),
 - 1.8. prawo do niepodlegania decyzjom opartym na zautomatyzowanym przetwarzaniu (art. 22 RODO).
2. Procedura realizacji praw osób, których dane dotyczą stanowi Załącznik nr 5 do Regulaminu.

10. OCHRONA DANYCH OSOBOWYCH W FAZIE PROJEKTOWANIA ORAZ DOMYŚLNA OCHRONA DANYCH OSOBOWYCH

1. Administrator Danych wdraża odpowiednie środki techniczne i organizacyjne, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, nadania przetwarzaniu danych niezbędnych zabezpieczeń oraz zapewnieniu ochrony praw osób, których dane dotyczą.
2. Wdrażając odpowiednie środki techniczne i organizacyjne Administrator Danych uwzględnia:
 - 2.1. stan wiedzy technicznej,
 - 2.2. koszt wdrażania,
 - 2.3. charakter, zakres, kontekst i cele przetwarzania danych,
 - 2.4. ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania.
3. Administrator Danych wdraża takie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia określonego celu przetwarzania, biorąc pod uwagę: ilość zbieranych danych osobowych, ich zakres, okres ich przechowywania oraz ich dostępność dla innych osób.
4. W szczególności stosowane środki techniczne i organizacje muszą zapewnić, by domyślnie dane osobowe nie były udostępniane nieokreślonej liczbie osób.
5. W pierwszej kolejności, Administrator Danych rozważa, czy cel jakiego ma służyć projektowane rozwiązanie jest możliwy do osiągnięcia bez konieczności przetwarzania danych osobowych. Jeśli tak, należy wybrać takie rozwiązanie.
6. Administrator Danych zapewnia, aby spełnienie warunków wskazanych w pkt 1-5 (tzw. zasady *privacy by design* i *privacy by default*) było odpowiednio udokumentowane np. w formie notatki, maila, raportu z przeprowadzonych testów systemu informatycznego, wydruku z ekranu systemu.
7. Ogólny opis organizacyjnych środków bezpieczeństwa wdrożonych w strukturze Administratora Danych stanowi Załącznik nr 6 do Regulaminu.

11. OCENA SKUTKÓW DLA OCHRONY DANYCH OSOBOWYCH (*DATA PROTECTION IMPACT ASSESSMENT*)

1. Administrator Danych dokonuje oceny skutków dla ochrony danych w celu opisanie przetwarzania danych osobowych oraz oceny jego konieczności i proporcjonalności, a także w celu wspomaganie zarządzania ryzykiem naruszenia praw i wolności osób fizycznych wynikającym z przetwarzania ich danych osobowych.
2. W strukturze Administratora Danych ocena skutków dla ochrony danych osobowych stanowi narzędzie rozliczalności ułatwiające przestrzeganie wymogów określonych w RODO, a także wykazanie, że podjęto odpowiednie środki w celu zapewnienia przestrzegania przepisów RODO.
3. Procedura oceny skutków dla ochrony danych osobowych (*data protection impact assessment*) stanowi Załącznik nr 8 do Regulaminu.

12. INCYDENTY OCHRONY DANYCH OSOBOWYCH

1. Osobami odpowiedzialnymi za bezpieczeństwo danych osobowych, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do pomieszczeń oraz systemów, w których przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia incydentów ochrony danych osobowych, jest: Administrator Danych, IOD oraz ASI (w odniesieniu do danych przetwarzanych w systemach informatycznych).
2. Procedura postępowania z incydentami ochrony danych osobowych stanowi Załącznik nr 4 do Regulaminu.

13. OGÓLNE ZASADY BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH

1. Dostęp do danych osobowych mogą mieć tylko pracownicy posiadający upoważnienie do ich przetwarzania.
2. Przebywanie osób nieuprawnionych do przetwarzania danych w pomieszczeniu, w którym przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do ich przetwarzania, chyba, że dane te są w odpowiedni sposób zabezpieczone przed dostępem.
3. Pracownicy mający dostęp do danych osobowych nie mogą ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem, w zakresie obowiązków służbowych, w ramach udzielonego upoważnienia do przetwarzania danych.
4. Pracownicy przechowujący dane osobowe zobowiązani są do zabezpieczenia materiałów zawierających dane w sposób uniemożliwiający dostęp do nich osobom nieuprawnionym.
5. Niedopuszczalnym jest wnoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia oraz jej bezpośredni przełożony.
6. Nikomu nie należy udostępniać indywidualnych haseł i identyfikatorów do systemów informatycznych.
7. Wysyłanie seryjnych wiadomości e-mail wymaga zastosowania opcji *kopia ukryta*.
8. Nie można udzielać informacji dotyczących danych osobowych innym podmiotom na podstawie prośby o takie dane skierowanej w formie zapytania telefonicznego.
9. W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej pracownicy zobowiązani są do stosowania zasady tzw. *czystego biurka*, która oznacza niepozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym. Za realizację powyższej zasady odpowiedzialny jest na swym stanowisku każdy z pracowników. Nie należy pozostawiać danych osobowych w miejscach ogólnodostępnych takich jak np. biurka, blaty, parapety.
10. Niszczanie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe odbywać się musi w sposób uniemożliwiający odczytanie zawartej w nich treści, np. z wykorzystaniem niszczarek.
11. Za bezpieczeństwo przetwarzania danych osobowych w określonym zbiorze indywidualną odpowiedzialność ponosi przede wszystkim każdy pracownik mający dostęp do danych.

12. W czasie chwilowej nieobecności pracowników w pomieszczeniach, w godzinach pracy jak i po zakończeniu pracy, są oni zobowiązani do zamykania na klucz pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe.
13. Klucze do pomieszczeń, w których przetwarzane są dane osobowe nie mogą być pozostawione w zamku w drzwiach. Pracownicy zobowiązani są do dołożenia należytej staranności w celu zabezpieczenia kluczy przed udostępnieniem ich osobom nieupoważnionym.
14. Przed wyjściem z pomieszczenia, w którym przechowywane są dane osobowe należy upewnić się, że zostało ono odpowiednio zabezpieczone (zamknięte okna, drzwi).
15. Po zakończeniu pracy w systemie informatycznym, w którym przechowywane są dane osobowe, należy wylogować się z systemu.
16. Osoba użytkująca komputer przenośny zawierający dane osobowe zobowiązana jest do zachowania szczególnej ostrożności podczas jego transportu, przechowywania i użytkowania poza obszarem, w którym przetwarzane są dane osobowe.
17. Na pracowniku pracującym zdalnie spoczywa obowiązek odpowiedniego zabezpieczenia danych tak, aby osoby trzecie nie miały dostępu do danych osobowych.
18. Dane osobowe przesyłane elektronicznie powinny być zabezpieczone hasłem. Hasło to powinno być wysyłane oddzielnym kanałem telekomunikacyjnym.

14. PRZEGLĄDY I AKTUALIZACJA POLITYKI OCHRONY DANYCH OSOBOWYCH

1. Regulamin podlega okresowemu przeglądowi pod kątem jej adekwatności, nie rzadziej niż raz do roku.
2. Przeglądu postanowień Regulaminu dokonuje IOD
3. Przegląd powinien obejmować, w szczególności ocenę adekwatności Polityki do:
 - 3.1. procesów funkcjonujących w strukturach Administratora Danych,
 - 3.2. obowiązujących przepisów prawa odnoszących się do ochrony danych osobowych, którym podlega Administrator Danych.
4. W każdym przypadku, gdy zmianie ulegają przepisy prawa będące źródłem wskazanych w Regulaminie obowiązków lub zaistnieją istotne zmiany faktyczne w ramach struktury Administratora Danych przegląd Regulaminu wykonywany jest niezwłocznie.
5. Jeżeli w wyniku przeglądu postanowień Regulaminu stwierdzona zostanie konieczność aktualizacji jego zapisów, IOD zaleca dokonanie aktualizacji stosownych postanowień Regulaminu w wymaganym zakresie.

15. ZAŁĄCZNIKI

Załącznik nr 1	Wzór upoważnienia pracownika do przetwarzania danych osobowych
Załącznik nr 2	Wzór ewidencji pracowników posiadających upoważnienie do przetwarzania danych osobowych
Załącznik nr 3	Wzór wykazu zbiorów danych osobowych wraz z procesami przetwarzania danych osobowych
Załącznik nr 4	Procedura postępowania z incydentami ochrony danych osobowych
Załącznik nr 5	Procedura realizacji praw osób, których dane dotyczą
Załącznik nr 6	Ogólny opis organizacyjnych i technicznych środków bezpieczeństwa
Załącznik nr 7	Zasady retencji danych osobowych
Załącznik nr 8	Procedura oceny skutków dla ochrony danych osobowych (<i>data protection impact assessment</i>)

Dokument sporządzono:	Pełen podpis Administratora Danych:	Pieczęć
Data:		
Miejsce:		

....., dn. 20r.

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art.29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s..1) – dalej **RODO** – nadaję upoważnienie Pani/Panu:

.....
(imię i nazwisko)
pełniącego stanowisko

.....
(stanowisko)
do przetwarzania danych osobowych w zakresie pełnionych obowiązków służbowych na zajmowanym stanowisku, tj. uzyskuje Pani/Pan upoważnienie do przetwarzania danych osobowych na Poziomie[wpisać kat. danych osobowych].
Upoważnienie obejmuje uprawnienie do przetwarzania danych osobowych dostępnych w zasobach Czeladzkiej Spółdzielni Mieszkaniowej w Czeladzi w okresie zatrudnienia, bez prawa dostępu do innych kategorii danych osobowych.

Jednocześnie zobowiązuję Panią/Pana do przetwarzania danych osobowych, zgodnie z udzielonym upoważnieniem oraz z przepisami RODO, ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, Kodeksu pracy, a także regulaminu ochrony danych osobowych Czeladzkiej Spółdzielni Mieszkaniowej w Czeladzi. Niniejsze upoważnienie uprawnia Panią/Pana do tworzenia/posiadania dla potrzeb wykonywanej pracy zestawień ewidencji oraz rejestrów z danymi osobowymi, z zachowaniem pełnej ich ochrony, przy zastosowaniu środków technicznych i organizacyjnych wdrożonych w Czeladzkiej Spółdzielni Mieszkaniowej w Czeladzi.

Okres ważności

od:

do:

.....
*podpis osoby
uprawnionej
do nadania
upoważnienia*

Data wygaśnięcia*
Odwołano, dnia

* Data rozwiązania stosunku pracy/umowy cywilnoprawnej.

Zakres danych osobowych wchodzących w skład poszczególnych poziomów upoważnień do przetwarzania danych osobowych:

Poziom 1 – dane osobowe klientów Administratora¹ tj. (imię nazwisko, numer telefonu, adres położenia lokalu mieszkalnego lub lokalu użytkowego znajdującego się w zasobach zarządzanych przez Administratora).

Poziom 2 – dane osobowe obejmujące Poziom 1, oraz pozostałe dane osobowe klientów Administratora tj. (stan cywilny, datę i miejsce urodzenia, imiona rodziców, nazwisko rodowe matki, nr dowodu osobistego, numer PESEL, kontaktowy numer telefoniczny, adres e-mail w przypadku wyrażenia zgody na odbiór korespondencji drogą elektroniczną, numer członkowski w przypadku posiadania członkostwa w Czeladzkiej Spółdzielni Mieszkaniowej, adres zameldowania, adres zamieszkania, informacje o ograniczonych prawach rzeczowych, cenie i sposobie nabycia, tytule prawnym do lokalu mieszkalnego, nr księgi wieczystej, nr ewidencyjny nieruchomości w skład której wchodzi lokal mieszkalny, informacje o cenie nabycia lokalu mieszkalnego, numer rachunku bankowego, informacje o trwających postępowaniach sądowych w których klient jest stroną).

Poziom 3 – dane osobowe pracowników Administratora w tym osób współpracujących oraz osób pełniących funkcje z wyboru tj. (imię, nazwisko, nazwisko rodowe, adres zamieszkania, numer członkostwa w przypadku posiadania członkostwa w Czeladzkiej Spółdzielni Mieszkaniowej w Czeladzi, numer telefonu, numer rachunku bankowego, stanowisko pracy, nazwę pełnionej funkcji, wymiar czasu pracy, wysokość wynagrodzenia lub diety, datę rozpoczęcia i zakończenia stosunku pracy, pełnienia funkcji z wyboru lub powołania, status osoby ubezpieczonej, numer PESEL).

Poziom 4 – dane osobowe obejmujące Poziom 1, Poziom 2 i Poziom 3.

¹ Członkowie i osoby nie posiadające członkostwa w CzSM w Czeladzi, posiadające tytuł prawny do lokalu mieszkalnego lub lokalu użytkowego w tym osoby wspólnie z nimi zamieszkujące, osoby fizyczne i osoby prawne współpracujące z Administratorem na podstawie odrębnego stosunku zobowiązaniowego w tym osoby wykonujące czynności powierzone w ich imieniu.

Zał. nr 2 do Regulaminu Ochrony Danych Osobowych CzSM w Czeladzi

PROCEDURA POSTĘPOWANIA Z INCYDENTAMI OCHRONY DANYCH OSOBOWYCH

1. W przypadku powzięcia przez pracownika Administratora, informacji o wykorzystaniu danych osobowych administrowanych przez Administratora niezgodnie z zasadami ich przetwarzania lub wystąpienia incydentu mogącego skutkować naruszeniem ochrony danych osobowych administrowanych przez Administratora, jest on zobowiązany bez zbędnej zwłoki do sporządzenia notatki służbowej opisującej szczegółowo dane zdarzenie oraz do poinformowania o zaistniałym incydencie IOD Administratora.
2. W zakresie wystąpienia incydentów naruszenia ochrony danych osobowych, które zostały wykryte przez podmiot przetwarzający dane osobowe w związku z ich powierzeniem, zasady postępowania są określone zapisami odrębnej umowy dotyczącej powierzenia danych osobowych od przetwarzania.
3. IOD po otrzymaniu zgłoszenia opisanego w ust. 1 dokonuje analizy zdarzenia celem stwierdzenia czy wypełnia ono przesłanki z art. 33 RODO.
4. W przypadku oceny pozytywnej IOD bez zbędnej zwłoki - w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia - zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin, IOD dołącza się wyjaśnienie przyczyn opóźnienia.
5. Zgłoszenie, o którym mowa w ust. 4, musi co najmniej:
 - a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
 - b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
 - c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
 - d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
6. Jeżeli i w zakresie, w jakim informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki
7. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.

PROCEDURA REALIZACJI PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ

1. W przypadku stwierdzenia przez IOD Administratora wystąpienia incydentu skutkującego naruszeniem ochrony danych osobowych osób fizycznych przetwarzanych przez Administratora, powodującego wysokie ryzyko naruszenia praw lub wolności tych osób, Administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

2. Zawiadomienie, o którym mowa w ust. 1 niniejszego artykułu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b), c) i d) RODO tj.

a) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;

b) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;

c) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

3. Zawiadomienie, o którym mowa w ust. 2, nie jest wymagane, w następujących przypadkach:

a) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

b) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,

c) wymagałoby ono niewspółmiernie dużego wysiłku.

4. W przypadku wystąpienia przesłanki z pkt. 3 ust. c), Administrator wydaje publiczny komunikat lub zastosować podobny środek przekazu informacji, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

OGÓLNY OPIS ORGANIZACYJNYCH I TECHNICZNYCH ŚRODKÓW BEZPIECZEŃSTWA

1. W celu wypełnienia zakresu obowiązków wynikających z postanowień art.24 i art. 32 RODO, Administrator w miejscu przetwarzania danych osobowych stosuje następujące organizacyjne środki bezpieczeństwa:
 - a) stosowanie upoważnień do przetwarzania danych osobowych przez pracowników Administratora;
 - b) stosowanie umów powierzenia danych osobowych do przetwarzania w przypadku przekazywania danych osobowych podmiotom trzecim;
 - c) stały nadzór IOD Administratora i AIS Administratora nad przestrzeganiem zasad ochronnych danych osobowych zgodnie z obowiązującymi regulacjami prawnymi oraz z obowiązującym Regulaminem Ochrony Danych Osobowych;
 - d) prowadzenie rejestru osób które pobierają klucze do pomieszczeń w których przechowywane są nośniki danych osobowych. Dostęp do kluczy mają wyłącznie osoby upoważnione do przetwarzania danych osobowych;
 - e) obowiązek zamykania przez pracowników Administratora kluczy do szaf w których przechowywane są nośniki danych w szyfrowanych sejfach. Kod dostępu do sejfu jest przydzielany każdemu pracownikowi indywidualnie;
 - f) obowiązek zamykania pomieszczeń w których przechowywane są nośniki danych osobowych w przypadku ich opuszczania przez pracownika;
 - g) obowiązek przebywania co najmniej jednego pracownika Administratora w pomieszczeniu w którym dochodzi do spotkania z klientami Administratora;
 - h) obowiązek utrzymywania zasady tzw. „ czystego biurka” tj. nie przechowywania w czasie i miejscu spotkania z klientami Administratora nośników danych osobowych które nie są przedmiotowo związane z odbywanym spotkaniem, a które zawierają chronione dane osobowe przetwarzane przez Administratora;
 - i) stosowanie ochrony komputerów osobistych służących do pracy poprzez przydzielenia hasła każdemu pracownikowi Administratora indywidualnie wraz z obowiązkiem wylogowania się z komputera przy każdorazowym opuszczeniu stanowiska pracy;
 - j) stosowanie ochrony dostępu do systemu zarządzania danymi Unisoft poprzez przydzielenia hasła każdemu pracownikowi Administratora indywidualnie wraz z obowiązkiem wylogowania się z systemu przy każdorazowym opuszczeniu stanowiska pracy;
 - k) stosowanie uwierzytelniania adresów poczty elektronicznej klientów Administratora przed dokonaniem przesłania tą drogą informacji chronionej;
 - l) stosowanie szyfrowania dokumentów przesyłanych przez Administratora drogą elektroniczną w formie załącznika;
 - m) stosowanie uwierzytelnianego dostępu dla użytkowników korzystających z modułu E-BOK;
 - n) zakaz wynoszenia nośników danych osobowych poza miejsce świadczenia pracy przez pracownika Administratora, chyba że są one niezbędne do wykonania czynności służbowych.
 - o) wyłączne uprawnienie do udostępniania danych osobowych przetwarzanych przez Administratora tylko osobom fizycznym i prawnym oraz organom administracji do tego uprawnionym;

- p) wyłączone uprawnienie do udostępniania danych osobowych przetwarzanych przez Administratora pomiędzy pracownikami Administratora i osobami współpracującymi tylko w przypadku posiadania przez obie osoby tego samego lub wyższego stopnia upoważnienia do przetwarzania danych osobowych z uwzględnieniem stopnia podporządkowania w schemacie organizacyjnym Administratora;
 - q) obowiązek niszczenia nośników danych zawierających dane osobowe przy użyciu certyfikowanych urządzeń niszczących;
 - r) dokonywanie regularnego niszczenia nośników danych zawierających dane osobowe oraz usuwania danych osobowych archiwizowanych w pamięci komputerowej oraz serwerach, w stosunku do których zakończył się okres retencji danych wynikający z obowiązującego stanu prawnego;
2. Administrator w miejscu przetwarzania danych osobowych stosuje następujące techniczne środki bezpieczeństwa:
- a. dostęp do obiektów i pomieszczeń w których przechowywane są nośniki danych osobowych, chroniony jest poprzez zamykanie obiektów, ochronę fizyczną obiektów świadczoną przez certyfikowany podmiot świadczący usługi ochrony osób i mienia, ochronę zdalną w postaci monitoringu wizyjnego i zainstalowanych systemów alarmowych świadczoną przez certyfikowany podmiot świadczący usługi ochrony osób i mienia;
 - b. dostęp do każdego pomieszczenia w którym przechowywane są nośniki danych jest chroniony jest poprzez ich zamykanie;
 - c. dostęp do każdej szafy w której przechowywane są nośniki danych zawierające dane osobowe chroniony jest poprzez ich zamykanie;
 - d. dostęp do komputerów służbowych pracownikowi Administratora w którym przetwarzane są dane osobowe chroniony jest hasłem;
 - e. każdy komputer w którym przetwarzane są dane osobowe, posiada oprogramowanie aktualizowane na bieżąco, jest zabezpieczony przez dostępem z sieci oprogramowaniem antywirusowym oraz zaporą elektroniczną typu firewall;
 - f. sieć wewnętrzna oraz sieć internetowa jest zabezpieczona oprogramowaniem antywirusowym oraz zaporą elektroniczną typu firewall;
 - g. dostęp do serwerów danych przetwarzających dane sieciowe z sieci wewnętrznej administratora jest chroniony poprzez zamykanie pomieszczeń w których są zamontowane;

ZASADY RETENCJI DANYCH OSOBOWYCH

1. Stosownie do postanowienia art. 5 RODO, Administrator przetwarza dane osobowe zgodnie z poniższymi zasadami:
 - a. przetwarza dane osobowe zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą ("zgodność z prawem, rzetelność i przejrzystość");
 - b. dane osobowe zbierane są konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane ("minimalizacja danych");
 - c. administrator dochowuje należytej staranności aby dane osobowe były prawidłowe i w razie potrzeby uaktualniane oraz podejmuje wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane ("prawidłowość");
 - d. dane osobowe przechowywane są w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane;
 - e. dane osobowe są przechowywane przez okres wynikający z przepisów ustawy prawo spółdzielcze z dnia 16 września 1982r., ustawy o spółdzielniach mieszkaniowych z dnia 15 grudnia 2000r., ustawy o własności lokali z dnia 24 czerwca 1994r., ustawy o odpadach z dnia 14 grudnia 2012r., ustawy o rachunkowości z dnia 29 września 1994r., ustawy kodeks cywilny z dnia 23 kwietnia 1964r., ustawy o podatku dochodowym od osób fizycznych z dnia 26 lipca 1991r., ustawa o podatku dochodowym od osób prawnych z dnia 15 lutego 1992r., ustawa o podatku od towarów i usług z dnia 11 marca 2004r.;
 - f. dane osobowe są przetwarzane przez okres dłuższy niż wynikający z ust. e), o ile są przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że administrator wdraża odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą ("ograniczenie przechowywania");
 - g. dane osobowe są przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych ("integralność i poufność");
 - h. administrator utrzymuje środki organizacyjne pozwalające wykazać przestrzeganie wyżej wskazanych zasad ("rozliczalność").

PROCEDURA OCENY SKUTKÓW DLA OCHRONY DANYCH OSOBOWYCH (DATA PROTECTION IMPACT ASSESSMENT)

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, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.
2. Dokonując oceny skutków dla ochrony danych, administrator konsultuje się z inspektorem ochrony danych, jeżeli został on wyznaczony.
3. Ocena skutków dla ochrony danych, o której mowa w ust. 1, 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, o których mowa w art. 9 ust. 1, lub danych osobowych dotyczących wyroków skazujących i czynów zabronionych, o czym mowa w art. 10;
 - c. systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.
4. Ocena zawiera co najmniej:
 - a. systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie - prawnie uzasadnionych interesów realizowanych przez administratora;
 - b. ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
 - c. ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, o którym mowa w ust. 1;
 - d. środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.
5. Oceniając - w szczególności do celów oceny skutków dla ochrony danych - skutki operacji przetwarzania wykonywanych przez administratora lub podmiot przetwarzający, uwzględnia się przestrzeganie przez takiego administratora lub taki podmiot przetwarzający zatwierdzonych kodeksów postępowania;
6. W stosownych przypadkach administrator zasięga opinii osób, których dane dotyczą, lub ich przedstawicieli w sprawie zamierzonego przetwarzania, bez uszczerbku dla ochrony interesów handlowych lub publicznych lub bezpieczeństwa operacji przetwarzania;