Uchwała nr 28/2026
Zarządu KSM „Nasz Dom" w Koszalinie z dnia 26 maja 2026 r.
w sprawie przyjęcia Polityki ochrony danych osobowych oraz Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w KSM „Nasz Dom" w Koszalinie

Na podstawie 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 (Dz. Urz. UE L 119, s. 1), Zarząd Spółdzielni postanowił, co następuje:

§ 1

Przyjąć Politykę ochrony danych osobowych do stosowania w KSM „Nasz Dom" w Koszalinie, stanowiącą załącznik nr 1 do uchwały.

§ 2

Przyjąć Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w KSM „Nasz Dom" w Koszalinie stanowiącą załącznik nr 2 do uchwały.

§ 3

1. Uchwała wraz z załącznikami podlega przekazaniu pracownikom Spółdzielni pocztą elektroniczną, a pracownikom nieobsługującym poczty elektronicznej w formie papierowej.

§ 4

1. Traci moc Polityka bezpieczeństwa danych osobowych w KSM „Nasz Dom" w Koszalinie przyjęta uchwałą Zarządu nr 33/2018 z 19 czerwca 2018 roku.
2. Traci moc Instrukcja Zarządzania Systemami Informatycznymi służącymi do przetwarzania danych osobowych w KSM „Nasz Dom" w Koszalinie przyjęta uchwałą Zarządu nr 33/2018 z 19 czerwca 2018 roku.

§ 5

Uchwała wchodzi w życie z dniem podjęcia.

PREZES ZARZĄDU
KSM „Nasz Dom"
mgr inż. Jacek Jańczewski

ZASTĘPCA PREZESA ZARZĄDU
ds. ekonomiczno-finansowych
GŁÓWNY KSIĘGOWY
mgr Ewelina Kowalska

Zarząd Spółdzielni

Załącznik Nr 1 do uchwały nr 29/2026
Zarządu KSM „Nasz Dom" w Koszalinie
z dnia 26 maja 2026 roku

Polityka ochrony danych osobowych			
Wydanie: 1.0	Data:26.05.2026	Zatwierdził:	Podpis:

ZASTĘPCA PREZESA ZARZĄDU
ds. ekonomiczno-finansowych
GŁÓWNY KSIĘGOWY
mgr Ewelina Kowalska

PREZES ZARZĄDU
KSM „Nasz Dom"
mgr inż. Jacek Janczewski

Koszalińska Spółdzielnia Mieszkaniowa „NASZ DOM"

Polityka ochrony danych osobowych

Niniejszy dokument jest Polityką Ochrony Danych Osobowych w rozumieniu RODO – 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 (Dz. Urz. UE L 119, s.1).

Zawiera on:

a) opis zasad ochrony danych obowiązujących u Administratora,
b) odwołania do procedur i instrukcji dotyczących poszczególnych obszarów ochrony danych osobowych.

Polityka Ochrony Danych Osobowych została sporządzona w celu wykazania, że dane osobowe są przetwarzane i zabezpieczone zgodnie z wymaganiami oraz zapewnienia zgodności z:

a) RODO,
b) Ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych.

Odpowiedzialny za wdrożenie i utrzymanie niniejszej Polityki jest Zarząd Koszalińskiej Spółdzielni Mieszkaniowej „NASZ DOM". Za nadzór i monitorowanie przestrzegania Polityki odpowiada Inspektor Ochrony Danych. Do stosowania Polityki zobowiązani są wszyscy pracownicy, którzy w zakresie swoich obowiązków służbowych mają przetwarzanie danych osobowych, jak również inne osoby, które z upoważnienia Administratora Danych uzyskały dostęp do danych osobowych.

§ 1 Skróty i definicje

Stosowane w niniejszym dokumencie skróty i definicje oznaczają:

a) Polityka oznacza niniejszą Politykę Ochrony Danych Osobowych, o ile co innego nie wynika wyraźnie z kontekstu.
b) RODO oznacza rozporządzenie 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).
c) Administrator danych (dalej Administrator) oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Administratorem Danych przetwarzanych w Koszalińska Spółdzielnia Mieszkaniowa „NASZ DOM".
d) Dane osobowe oznaczają wszystkie informacje dotyczące zidentyfikowanych lub możliwych do zidentyfikowania osób fizycznych (pełną definicję zawiera art. 4 ust. 1 RODO).
e) Dane wrażliwe oznaczają dane szczególne i dane dotyczące wyroków skazujących i naruszeń prawa.
f) Dane szczególne oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej.
g) Osoba oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu.
h) Podmiot przetwarzający oznacza organizację lub osobę, której Administrator Danych powierzył przetwarzanie danych osobowych (np. osoba lub firma obsługująca Administratora Danych w zakresie BHP),
i) Profilowanie oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy

tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się,

j) Eksport danych oznacza przekazanie danych do państwa trzeciego lub organizacji międzynarodowej.

k) IOD lub Inspektor oznacza Inspektora Ochrony Danych Osobowych.

l) RCPD lub Rejestr oznacza Rejestr Czynności Przetwarzania Danych.

§ 2 Inspektor Ochrony Danych

1. Administrator nie ma obowiązku powołania Inspektora Ochrony Danych (IOD), ale uczynił to na podstawie art. 37 ust. 4 RODO.
2. Osoba powołana na stanowisko IOD posiada:
   a) odpowiednią wiedzę fachową tj. gruntowną wiedzę na temat krajowego i europejskiego prawa oraz praktyk w dziedzinie ochrony danych osobowych,
   b) znajomość struktury administratora oraz wiedzę o dokonywanych czynnościach przetwarzania a także o systemach informatycznych oraz o potrzebach administratora w zakresie bezpieczeństwa i ochrony danych,
   c) znajomość przepisów administracyjnych oraz postępowania administracyjnego w jednostce organizacyjnej,

   i odpowiednie cechy osobowe tj. uczciwość i wysoko rozwiniętą etykę zawodową.
3. IOD jest zatrudniony na podstawie umowy cywilno-prawnej i został powołany dokumentem „Wyznaczenie Inspektora Ochrony Danych".
4. IOD wykonuje obowiązki wskazane w art. 39 RODO.

§ 3 Zasady ochrony przetwarzania danych osobowych

Administrator przetwarza dane osobowe z poszanowaniem następujących zasad:

1. w oparciu o podstawę prawną i zgodnie z prawem,
2. rzetelnie i uczciwie,
3. w sposób przejrzysty dla osoby, której dane dotyczą,
4. w konkretnych celach,
5. tylko niezbędne dane,
6. nie dłużej niż trzeba,
7. zapewniając odpowiednie bezpieczeństwo danych.

§ 4 System ochrony danych

Na system ochrony danych osobowych składają się następujące elementy:

1. zidentyfikowane zbiory danych osobowych oraz opis ich przetwarzania,
2. Rejestr Czynności Przetwarzania Danych Osobowych,
3. podstawy prawne przetwarzania danych osobowych,
4. zasady realizacji obowiązku informacyjnego,
5. procedury obsługi praw osób, których dane są przetwarzane,
6. metody zarządzania minimalizacją przetwarzanych danych,
7. procedury zapewniające odpowiedni poziom bezpieczeństwa danych,
8. zasady identyfikacji i obsługi incydentów,
9. procedura przywrócenia dostępności danych osobowych w razie wystąpienia incydentu,
10. zasady powierzania przetwarzania danych podmiotom zewnętrznym,

11. zasady uruchamiania nowych projektów, w ramach których będą przetwarzane dane osobowe.

4.1. Identyfikacja zbiorów danych osobowych

Administrator danych zidentyfikował procesy i zbiory, w których są przetwarzane dane osobowe. Dla każdego zbioru wskazano właściciela i zweryfikowano czy nie zachodzi przypadek współadministrowania. W ramach przeprowadzonej inwentaryzacji zostały wskazane grupy informacji przetwarzane w zbiorach. W ramach każdego zbioru dokonano analizy związanej z przetwarzaniem szczególnych kategorii danych osobowych oraz ewentualnym profilowaniem.

Zinwentaryzowane zbiory zostały opisane w „Rejestrze Czynności Przetwarzania Danych Osobowych".

4.2. Rejestr Czynności Przetwarzania Danych Osobowych

Administrator danych prowadzi, zgodnie z wymaganiami art. 30 RODO, Rejestr Czynności Przetwarzania Danych Osobowych. Rejestr stanowi formę dokumentowania czynności przetwarzania danych osobowych. Za prowadzenie Rejestru odpowiada IOD we współpracy z właścicielami zbiorów. Rejestr jest aktualizowany w przypadku podjęcia przez Administratora nowych czynności przetwarzania danych, zaprzestania realizacji opisanej wcześniej czynności lub zmian w opisie istniejącej czynności. Za wnioskowanie o aktualizację Rejestru Czynności Przetwarzania odpowiada właściciel zbioru. Wzór Rejestru Czynności Przetwarzania Danych stanowi zał. nr 1 do Polityki.

Niektóre dane osobowe są przetwarzane przez Administratora na podstawie umowy powierzenia przetwarzania. Rejestr dla tych danych prowadzony jest zgodnie ze wzorem stanowiącym zał. nr 2 do Polityki.

4.3. Podstawy prawne przetwarzania danych osobowych

Administrator dokumentuje w Rejestrze Czynności Przetwarzania, o którym mowa w pkt. 4.2. podstawy prawne przetwarzania danych osobowych dla poszczególnych zbiorów. W przypadku każdego zbioru wskazuje podstawę prawną przetwarzania danych zwykłych i szczególnych kategorii danych osobowych, które wynikają z RODO (np. zgoda, umowa czy obowiązek prawny) i dookreśla je dodatkowymi informacjami np. dla zgody wskazując na jej zakres a w przypadku podstawy prawnej konkretny przepis ustawy branżowej. Podstawy prawne są okresowo weryfikowane.

4.4. Zasady realizacji obowiązku informacyjnego

Przy pozyskiwaniu danych osobowych od osoby, której dane dotyczą Administrator spełnia obowiązek informacyjny opisany w art. 13 RODO.

W przypadku pozyskiwania danych od potencjalnych pracowników, Administrator przekazuje podstawowe informacje dotyczące przetwarzania danych w ogłoszeniu o rozpoczęciu rekrutacji lub przy przyjmowaniu CV.

Przy zbieraniu danych od pracowników, obowiązek informacyjny realizowany jest przez udostępnienie informacji o przetwarzaniu danych pracownika w formie dokumentu papierowego i potwierdzenie zapoznania się z nim przez złożenie podpisu pod stosownym oświadczeniem. W stosunku do osób zatrudnionych u Administratora w dniu wejścia w życie niniejszej Polityki obowiązek informacyjny został zrealizowany przez przekazanie klauzuli w formie elektronicznej lub papierowej.

W innych przypadkach pozyskiwania danych osobowych, podmiotom danych jest udostępniana stosowna klauzula informacyjna lub informacja w jaki sposób się z nią zapoznać na

formularzach, które służą do pozyskania danych osobowych. W tym wypadku klauzule informacyjne publikowane są na stronie internetowej administratora.

4.5. Procedury obsługi praw osób, których dane są przetwarzane

W celu właściwej obsługi praw osób, których dane są przetwarzane przez Administratora, została opracowana Procedura obsługi żądań podmiotu danych, która stanowi załącznik nr 3 do niniejszego dokumentu.

4.6. Metody zarządzania minimalizacją przetwarzanych danych

Na minimalizację przetwarzania danych mają wpływ następujące czynniki:

- adekwatność danych w stosunku do celu przetwarzania,

- dostęp do danych tylko dla tych osób i w takim zakresie jak jest to niezbędne,

- przechowywanie danych nie dłużej niż jest to niezbędne.

W ramach wdrażania RODO Administrator zweryfikował zakres pozyskiwanych informacji oraz zakres ich przetwarzania pod kątem adekwatności w stosunku do celu. Administrator zobowiązał właścicieli danych osobowych do okresowego przeglądu pozyskiwanych i przetwarzanych danych osobowych, by zapewnić, że ich zakres nie wykracza ponad niezbędne minimum. W celu wywiązania się z tego zadania, właściciel danych powinien między innymi zweryfikować, czy nie nastąpiły zmiany w przepisach prawa.

W celu minimalizacji dostępu do danych osobowych Administrator stosuje ograniczenia organizacyjne, fizyczne i informatyczne. Ograniczenia organizacyjne realizowane są poprzez nadawanie upoważnień do przetwarzania danych osobowych związanych z zajmowanym stanowiskiem. Ograniczenia fizyczne wynikają z reglamentacji dostępu do pomieszczeń i dokumentów. Ograniczenia informatyczne realizowane są przez nadawanie odpowiednich uprawnień dostępowych do zasobów sieciowych i systemów, w których są przetwarzane dane osobowe. Uprawnienia dostępowe są aktualizowane przy zmianie stanowiska lub roli pracownika w procesie przetwarzania danych. Administrator zapewnia, że przynajmniej raz do roku dokonuje przeglądu użytkowników systemów i nadanych im uprawnień. Szczegółowe zasady zarządzania uprawnieniami zostały opisane w Procedurze nadawania i zmiany uprawnień.

Administrator zarządza cyklem życia dokumentów. Jednolity Rzeczowy Wykaz Akt / Właściciel zbioru określa zarówno okres przechowywania dokumentów na stanowisku pracy jak i okres ich archiwizacji. Zasady retencji danych osobowych przekazywane są osobom, których dane dotyczą w Klauzuli informacyjnej. Administrator zapewnia, że dokumenty przechowywane w archiwum są poddawane okresowym przeglądom i że są niszczone w bezpieczny sposób po upływie okresu ich przechowywania.

4.7. Procedury zapewniające odpowiedni poziom bezpieczeństwa

Administrator zapewnia odpowiedni poziom bezpieczeństwa danych osobowych przez:

- Zapewnienie odpowiedniego stanu wiedzy o bezpieczeństwie i zagrożeniach wynikających z przetwarzania danych osobowych (szkolenia pracowników).

- Okresowe przeprowadzanie analizy ryzyka zgodnie z przyjętą Metodyką zarządzania ryzykiem i dobór możliwych do zastosowania zabezpieczeń organizacyjnych, fizycznych i informatycznych. (Wykaz wprowadzonych zabezpieczeń stanowi załącznik nr 4 do Polityki).

- Weryfikację skuteczności wdrożonych zabezpieczeń.

- Przeprowadzenie oceny skutków dla ochrony danych osobowych w tych operacjach, które zostały wskazane przez organ nadzorczy (Komunikat Prezesa Urzędu Ochrony Danych Osobowych opublikowany w Monitorze Polskim). Administrator jest zwolniony z przeprowadzania oceny skutków dla ochrony danych dla tych operacji przetwarzania, które mają podstawę prawną w prawie polskim lub prawie UE.

Po wdrożeniu nowych zabezpieczeń, ustanowionych w wyniku przeprowadzonej analizy ryzyka i ewentualnie oceny skutków dla ochrony danych osobowych dokument Wykaz stosowanych zabezpieczeń powinien zostać zaktualizowany. Za aktualizację opisu zabezpieczeń informatycznych odpowiada ASI.

4.8. Zasady identyfikacji i obsługi incydentów

Administrator przyjął zasady zobowiązujące wszystkich pracowników do powiadamiania o stwierdzeniu podatności systemu ochrony danych lub wystąpieniu incydentu bezpieczeństwa. Zasady te zostały opisane w Regulaminie ochrony danych osobowych (załącznik nr 8 do Polityki).

Zasady obsługi naruszeń ochrony danych zostały opisane w załączniku nr 5 do Polityki.

4.9. Zasady powierzania przetwarzania danych podmiotom zewnętrznym

Administrator opracował ankietę, na podstawie której weryfikuje firmy, z którymi zamierza podpisać umowy powierzenia przetwarzania danych osobowych (załącznik nr 6 do Polityki). Weryfikacja firm ma zapewnić, że podmioty przetwarzające dają wystarczające gwarancje bezpiecznego przetwarzania danych osobowych.

Administrator opracował wzór umowy powierzenia przetwarzania danych osobowych, który stanowi załącznik nr 7 do Polityki.

Administrator prowadzi rejestr umów, na podstawie których powierzył przetwarzanie danych podmiotom zewnętrznym.

4.11. Zasady uruchamiania nowych projektów, w ramach których będą przetwarzane dane osobowe

W przypadku uruchamiania nowych projektów związanych z przetwarzaniem danych osobowych administrator zapewnia, że uwzględnia w nich zagadnienia związane z bezpieczeństwem i minimalizacją przetwarzanych danych.

§ 5 Postanowienia końcowe

1. Każdy pracownik przed dopuszczeniem do przetwarzania danych osobowych jest przeszkolony w zakresie RODO i wewnętrznych regulacji dotyczących ochrony danych osobowych.
2. Zbiór podstawowych zasad bezpiecznego przetwarzania danych osobowych został zapisany w Regulaminie ochrony danych osobowych (zał. nr 8 do Polityki).
3. Po zapoznaniu się z zasadami ochrony danych osobowych, pracownik potwierdza znajomość tych zasad i deklaruje ich stosowanie.

Zał. nr 1 do Polityki

Rejestr Czynności Przetwarzania

Nazwa i dane kontaktowe Administratora Danych	
Nazwa zbioru / procesu	
Nazwa czynności przetwarzania	
Cele przetwarzania	
Realizacja obowiązku informacyjnego	
Kategorie osób, których dane dotyczą	
Kategorie danych osobowych	
Podstawa prawna	
Planowany termin usunięcia	
Kategorie odbiorców	
Kategorie odbiorców w państwach trzecich lub w organizacjach międzynarodowych	
Nazwa państwa trzeciego lub w organizacji międzynarodowej, do których następuje transfer (dokumentacja zabezpieczeń transferu)	
Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa	
Powierzenie przetwarzania	
System informatyczny	

Zał. nr 2 do Polityki

Rejestr Kategorii Czynności Przetwarzania

Nazwa oraz dane kontaktowe podmiotu przetwarzającego	
Dane IOD administratora	
Kategorie przetwarzań realizowane w imieniu administratora	
Przekazania danych osobowych do państwa trzeciego lub w organizacji międzynarodowej	
Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa	

Zał. nr 3 do Polityki

PROCEDURA OBSŁUGI ŻADAŃ PODMIOTU DANYCH

Procedura opisuje sposób postępowania Administratora danych w sytuacji, gdy osoba, której dane dotyczą skieruje do Administratora danych żądanie związane z realizacją jej praw, określonych w art. 15 – 18 i 20 - 21 RODO.

Żądanie związane z realizacją praw podmiotu danych może wpłynąć do Administratora danych w formie:
- tradycyjnej (papierowej) – na adres korespondencyjny,
- elektronicznej – na dedykowany adres IOD, adres sekretariatu lub dowolnej komórki organizacyjnej,
- ustnej – kierowanej do pracowników Administratora danych.

RODO nie precyzuje treści żądania. Każde żądanie, które wpłynęło do Administratora danych, niezależnie od formy, powinno trafić do IOD w celu jego zaewidencjonowania i rozpatrzenia. Rozpatrywanie żądań powinno być realizowane w oparciu o schematy postępowania, które stanowią załączniki do niniejszej procedury.

Gdy Administrator uzna, że żądania wnioskodawcy są ewidentnie nieuzasadnione bądź nadmierne, to może, działając zgodnie z art. 12 ust. 5 RODO:
- pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań, lub
- odmówić podjęcia działań w związku z żądaniem.
Na Administratorze ciąży wtedy obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter.

Działania niezbędne do rozpatrzenia i realizacji żądania wykonuje IOD przy wsparciu osób wskazanych przez Administratora danych. Propozycję odpowiedzi na żądanie dotyczące realizacji praw podmiotu danych zespół każdorazowo przedstawia Administratorowi do akceptacji. Wszystkie odpowiedzi są archiwizowane przez IOD.

Odpowiedź powinna być udzielona niezwłocznie, nie później niż w ciągu 30 dni od otrzymania żądania.

IOD zobowiązany jest do wykorzystania dostępnych środków w celu zweryfikowania tożsamości osoby zwracającej się z żądaniami dotyczącymi realizacji jej praw, zwłaszcza gdy żądanie skierowane było drogą elektroniczną.

Realizacja żądania na podstawie art. 15 RODO

Prawo dostępu do danych osobowych

1. Wniosek o udzielenie informacji

Z wnioskiem do Administratora danych o udzielenie informacji na temat przetwarzania danych osobowych może się zwrócić każda osoba, niezależnie od tego, czy Administrator takie dane przetwarza czy też nie.

Odpowiedź twierdząca Administratora danych może stanowić podstawę do realizacji praw wynikających z art. 16 – 18 i 20 - 21.

2. Sprawdzenie czy Administrator danych przetwarza dane osobowe wnioskodawcy

Administrator danych sprawdza, czy na jakimkolwiek etapie przetwarza dane osobowe wnioskodawcy (między innymi czy dane przechowuje w Zakładowej Składnicy Akt). Sprawdzeniu podlegają zarówno zbiory prowadzone w wersji papierowej jak i elektronicznej. W przypadku, gdy Administrator danych nie przetwarza danych osobowych wnioskodawcy, powinien o tym wnioskodawcę poinformować.

3. Sprawdzenie czy przepisy szczególne wyłączają obowiązek informacyjny

Obowiązek informacyjny może podlegać ograniczeniom wynikającym z przepisów szczególnych. Między innymi w art. 6 projektu Ustawy o ochronie danych osobowych przewidziane są wyjątki dotyczące realizacji obowiązku informacyjnego przez organy publiczne. Jeżeli taka sytuacja ma miejsce Administrator danych odmawia udzielenia informacji wskazując przepisy ustaw szczególnych, które wyłączają obowiązek informacyjny.

4. Wezwanie do udzielenia dodatkowych informacji

Art. 6 ust. 2 projektu Ustawy o ochronie danych osobowych, w przypadku wykonywania zadań publicznych, daje możliwość wezwania wnioskodawcy do udzielenia dodatkowych informacji pozwalających na wyszukanie danych osobowych. Dalsze kroki procedury realizowane będą po uszczegółowieniu wniosku.

5. Ocena czy żądania są ewidentnie nieuzasadnione lub nadmierne

Jeżeli Administrator danych stwierdzi, że żądania wnioskodawcy są ewidentnie nieuzasadnione lub nadmierne (musi to wykazać), to ma prawo skorzystać z art. 12 ust. 5 RODO i może pobrać rozsądną opłatę lub odmówić podjęcia działań w związku z żądaniem. W obu przypadkach Administrator danych powinien uwzględnić okoliczności faktyczne i rozważyć konsekwencje dokonania wyboru.

W przypadku odmowy podjęcia działań Administrator danych informuje o tym fakcie wnioskodawcę.

W przypadku skorzystania z możliwości pobrania rozsądnej opłaty Administrator wzywa wnioskodawcę do jej uiszczenia i dopiero po jej otrzymaniu podejmuje dalsze kroki.

6. Udzielenie informacji

Administrator danych potwierdza przetwarzanie danych wnioskodawcy i przygotowuje odpowiedź, która zawiera informacje opisane w art. 15 RODO.

Odpowiedź powinna być przekazana w taki sam sposób w jaki wpłynęło żądanie.

Realizacja żądania na podstawie art. 16 RODO

Prawo dostępu do danych osobowych

1. Wniosek o sprostowanie (skorygowanie, uzupełnienie) danych osobowych

Jeżeli osoba, której dane dotyczą, na podstawie uzyskanych od administratora informacji stwierdzi, że dane na jej temat są nieprawidłowe (nieaktualne, błędne, niekompletne), to może się zwrócić do Administratora danych z żądaniem ich sprostowania lub uzupełnienia. Podmiot danych musi okazać dokument potwierdzający prawidłowe i aktualne dane lub w inny sposób wykazać swoje roszczenia.

2. Sprawdzenie czy spełnienie żądania regulowane jest przepisami szczególnymi i czy jest zasadne

Administrator danych sprawdza, czy sprostowanie danych jest regulowane w obowiązujących go przepisach szczególnych. Na przykład oczywiste pomyłki w decyzjach administracyjnych prostuje organ, który je uczynił w drodze postanowienia, na które przysługuje zażalenie. W w/w przypadku nie można się powołać na przepisy RODO. Osobną kwestią pozostaje sprawdzenie, czy żądanie jest zasadne. Przy rozpatrywaniu zasadności wniosku, związanego z niekompletnością danych należy brać pod uwagę cele przetwarzania. Jeżeli zachodzi któraś z wymienionych przesłanek (sprostowanie danych regulują inne przepisy, żądanie jest nieuzasadnione) Administrator danych odmawia spełnienia żądania o czym informuje wnioskodawcę.

3. Spełnienie żądania

Jeżeli żądanie jest zasadne Administrator powinien je zrealizować i poinformować wnioskodawcę o sposobie realizacji żądania. Informacja powinna być przekazana niezwłocznie, nie później niż w terminie 30 dni od otrzymania żądania. Termin realizacji żądania, w razie potrzeby można przedłużyć o kolejne dwa miesiące w przypadku, kiedy jego realizacja ma skomplikowany charakter. Informację o przedłużeniu terminu realizacji żądania Administrator danych przekazuje wnioskodawcy w terminie 30 dni od złożenia wniosku. Jeżeli wniosek był przekazany w formie elektronicznej, to odpowiedź powinna być również przekazana w takiej formie, chyba że wnioskodawca wskazał inną formę komunikacji.

W przypadku, gdy Administrator danych udostępnił dane odbiorcy, powinien poinformować odbiorcę o dokonanym sprostowaniu danych, chyba że będzie to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.

Realizacja żądania na podstawie art.17 RODO

Prawo do usunięcia danych osobowych („Prawo do bycia zapomnianym")

1. Wniosek o usunięcie danych osobowych

Jeżeli osoba, której dane dotyczą:
- stwierdzi, że dane nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane,
- cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania,
- wnosi sprzeciw wobec przetwarzania jej danych,
- stwierdzi, że dane osobowe były przetwarzane niezgodnie z prawem,
- stwierdzi, że dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego, któremu podlega administrator,
- stwierdzi, że dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego tzw. usług internetowych,
to może żądać od Administratora danych ich usunięcia. Wnioskodawca musi wykazać nieprawidłowości, nielegalność przetwarzania lub zbędność danych.

2. Sprawdzenie czy spełnienie żądania jest zasadne

Administrator danych sprawdza, czy zachodzi któraś z przesłanek wskazanych w art. 17 ust. 1 RODO, która uprawnia do wniesienia żądania. Jeżeli, w ocenie Administratora danych, nie zachodzi żadna z przesłanek pozwalających na wniesienie żądania, to informuje on wnioskodawcę o niespełnieniu żądania i powodach takiej decyzji.

3. Sprawdzenie czy nie zachodzą przesłanki wyłączające zapisy art. 17 ust. 1 i 2 RODO

Administrator danych sprawdza, czy można wykazać, że przetwarzanie danych jest niezbędne:
- do korzystania z prawa do wolności wypowiedzi i informacji (prawo wolności wypowiedzi i informacji ma prymat w stosunku do RODO),
- do wywiązania się z prawnego obowiązku lub wykonania zadania realizowanego w interesie publicznym bądź w ramach sprawowania władzy publicznej (przesłanka może być wykorzystywana w przypadku Administratorów danych z sektora publicznego),
- z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego,
- do celów archiwalnych, badań naukowych, historycznych lub statystycznych,
- do ustalenia, dochodzenia lub obrony roszczeń.
Jeżeli zachodzi któraś z wyżej wymienionych przesłanek wyłączających Prawo do usunięcia danych osobowych, to Administrator danych informuje wnioskodawcę o niespełnieniu żądania i powodach takiej decyzji.

4. Informacja o spełnieniu żądania

Jeżeli żądanie jest uprawnione, to Administrator danych usuwa kwestionowane dane i informuje wnioskodawcę o sposobie realizacji żądania. Informacja powinna być przekazana niezwłocznie, nie później niż w terminie 30 dni od otrzymania żądania. Termin realizacji

żądania, w razie potrzeby można przedłużyć o kolejne dwa miesiące, w przypadku kiedy jego realizacja ma skomplikowany charakter. Informację o przedłużeniu terminu realizacji żądania Administrator danych przekazuje wnioskodawcy w terminie 30 dni od złożenia wniosku. Jeżeli wniosek był przekazany w formie elektronicznej, to odpowiedź powinna być również przekazana w takiej formie, chyba że wnioskodawca wskazał inną formę komunikacji.

W przypadku, gdy Administrator danych upublicznił dane osobowe, to uwzględniając dostępną technologię i koszty realizacji, podejmuje on rozsądne działania, by poinformować administratorów przetwarzających te dane osobowe, że podmiot danych żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, ich kopie i replikacje.

Realizacja żądania na podstawie art.18 RODO

Prawo do ograniczenia przetwarzania

1. Wniosek o ograniczenie przetwarzania danych osobowych

Jeżeli osoba, której dane dotyczą kwestionuje prawidłowość danych, może zwrócić się do Administratora z żądaniem ograniczenia przetwarzania danych na okres pozwalający administratorowi sprawdzić prawidłowość tych danych.
Żądanie takie podmiot danych może skierować do administratora również w przypadku, gdy:
- przetwarzanie jest niezgodne z prawem, a osoba której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
- administrator nie potrzebuje już danych osobowych do realizacji celu przetwarzania, ale są one potrzebne osobie, której dane dotyczą , do ustalenia, dochodzenia lub obrony roszczeń,
- osoba, której dane dotyczą wniosła sprzeciw wobec przetwarzania na mocy art., 21 ust. 1 RODO – do czasu stwierdzenia, czy prawnie uzasadnione podstawy prawne po stronie administratora są nadrzędne wobec podstaw prawnych sprzeciwu osoby, której dane dotyczą.

2. Sprawdzenie czy uprawnienie do żądania do ograniczenia przetwarzania zostało wyłączone na mocy przepisów szczególnych

Administrator danych sprawdza, czy ograniczenie przetwarzania danych jest regulowane w obowiązujących go przepisach szczególnych. W związku z wejściem RODO przewiduje się zmiany w dużej grupie przepisów szczególnych. Niektóre z nich będą wprowadzały wyłączenia wobec stosowania omawianego przepisu.

Jeżeli przepisy szczególne wprowadzają ograniczenia, to Administrator danych odmawia spełnienia żądania o czym informuje wnioskodawcę.

3. Sprawdzenie czy spełnienie żądania jest zasadne

Administrator danych sprawdza, czy zachodzi któraś z przesłanek wskazanych w art. 18 ust. 1 RODO, która uprawnia do wniesienia żądania. Jeżeli, w ocenie Administratora danych, nie zachodzi żadna z przesłanek pozwalających na wniesienie żądania, to informuje on wnioskodawcę o niespełnieniu żądania i powodach takiej decyzji.

4. Informacja o spełnieniu żądania

Jeżeli żądanie jest uprawnione, to Administrator danych je spełnia. Spełnienie żądania ograniczenia przetwarzania oznacza, że Administrator oznacza dane osobowe i przetwarzanie ogranicza do przechowywania. Administrator może przetwarzać dane w inny sposób wyłącznie za zgodą osoby której dane dotyczą albo w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.

Po spełnieniu żądania Administrator informuje wnioskodawcę o sposobie realizacji żądania. Informacja powinna być przekazana niezwłocznie, nie później niż w terminie 30 dni od otrzymania żądania. Termin realizacji żądania, w razie potrzeby można przedłużyć o kolejne dwa miesiące, w przypadku kiedy jego realizacja ma skomplikowany charakter. Informację o przedłużeniu terminu realizacji żądania Administrator danych przekazuje wnioskodawcy w terminie 30 dni od złożenia wniosku. Jeżeli wniosek był przekazany w formie elektronicznej, to odpowiedź powinna być również przekazana w takiej formie, chyba że wnioskodawca wskazał inną formę komunikacji.

W przypadku, gdy Administrator danych udostępnił dane osobowe odbiorcy, to powinien poinformować odbiorcę, któremu ujawniono dane, o ograniczeniu przetwarzania danych, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.

Realizacja żądania na podstawie art.20 RODO

Prawo do przenoszenia danych

1. Wniosek o przeniesienie danych osobowych

Prawo do przeniesienia danych osobowych ma ułatwić zmianę dostawcy usług.
Żądanie przeniesienia danych osobowych podmiot danych może skierować do Administratora danych jeżeli przetwarzanie realizowane jest na podstawie zgody osoby, której dane dotyczą lub umowy oraz gdy przetwarzanie odbywa się w sposób zautomatyzowany. Celem realizacji żądania jest zmiana dostawcy usług.

2. Sprawdzenie czy uprawnienie do żądania do przeniesienia danych zostało wyłączone na mocy przepisów szczególnych

Administrator danych sprawdza, czy prawo do przenoszenia danych jest regulowane w obowiązujących go przepisach szczególnych. W związku z wejściem RODO przewiduje się zmiany w dużej grupie przepisów szczególnych. Niektóre z nich będą wprowadzały wyłączenia wobec stosowania omawianego przepisu.

Jeżeli przepisy szczególne wprowadzają ograniczenia, to Administrator danych odmawia spełnienia żądania o czym informuje wnioskodawcę.

3. Sprawdzenie czy spełnienie żądania jest zasadne

Administrator danych sprawdza, czy zachodzą przesłanki wskazane w art. 20 ust. 1 RODO, które uprawniają do wniesienia żądania. Jeżeli, w ocenie Administratora danych, nie zachodzą przesłanki pozwalające na wniesienie żądania, to informuje on wnioskodawcę o niespełnieniu żądania i powodach takiej decyzji.

4. Informacja o spełnieniu żądania

Jeżeli żądanie jest uprawnione, to Administrator danych je spełnia. Spełnienie żądania przeniesienia danych oznacza, że Administrator przekazuje dane osobowe, które otrzymał od podmiotu danych, w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego osobie, której dane dotyczą lub innemu administratorowi, w zależności od żądania.

O realizacji żądania Administrator informuje wnioskodawcę. Informacja powinna być przekazana niezwłocznie, nie później niż w terminie 30 dni od otrzymania żądania. Termin realizacji żądania, w razie potrzeby można przedłużyć o kolejne dwa miesiące, w przypadku kiedy jego realizacja ma skomplikowany charakter. Informację o przedłużeniu terminu realizacji żądania Administrator danych przekazuje wnioskodawcy w terminie 30 dni od złożenia wniosku. Jeżeli wniosek był przekazany w formie elektronicznej, to odpowiedź powinna być również przekazana w takiej formie, chyba że wnioskodawca wskazał inną formę komunikacji.

Realizacja żądania na podstawie art.21 RODO

Prawo wniesienia sprzeciwu

1. Wniesienie sprzeciwu

Jeżeli osoba, której dane dotyczą, sprzeciwia się przetwarzaniu danych osobowych, może wnieść do Administratora sprzeciw.
Sprzeciw nie przysługuje, gdy:
- przetwarzanie danych osobowych odbywa się na podstawie zgody na przetwarzanie (w tym wypadku osoba powinna cofnąć zgodę),
- podstawą przetwarzania danych osobowych jest konieczność realizacji umowy,
- przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze,
- przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej.

2. Sprawdzenie czy uprawnienie do wniesienia sprzeciwu zostało wyłączone na mocy przepisów szczególnych

Administrator danych sprawdza, czy ograniczenie wniesienie sprzeciwu jest regulowane w obowiązujących go przepisach szczególnych. W związku z wejściem RODO przewiduje się zmiany w dużej grupie przepisów szczególnych. Niektóre z nich będą wprowadzały wyłączenia wobec stosowania omawianego przepisu.

Jeżeli przepisy szczególne wprowadzają ograniczenia, to Administrator danych odmawia spełnienia żądania o czym informuje wnioskodawcę.

3. Sprawdzenie czy spełnienie żądania jest zasadne na podstawie art. 21 ust. 1

Administrator danych sprawdza, czy żądanie wynika z przesłanek wymienionych w art. 21 ust. 1 i czy zachodzi któraś z nich, tj.:
- przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej,
- przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów Administratora lub strony trzeciej z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą jest dzieckiem.
Jeżeli, w ocenie Administratora danych, nie zachodzi żadna z przesłanek wymienionych w art. 21 ust. 1 pozwalających na wniesienie żądania, to informuje on wnioskodawcę o niespełnieniu żądania i powodach takiej decyzji.

4. Czy dane są przetwarzane na potrzeby marketingu bezpośredniego (art. 21 ust. 2)

Jeżeli Administrator przetwarza dane osobowe na potrzeby marketingu bezpośredniego, w tym profilowania, to osoba, której dane są przetwarzane ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzaniu danych w tym celu. Po wniesieniu sprzeciwu

administrator nie może już przetwarzać danych w tym celu, chyba że wykaże on istnienie ważnych, prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

5. Informacja o spełnieniu żądania

Jeżeli żądanie jest uprawnione, to Administrator danych je spełnia. Uwzględnienie sprzeciwu oznacza, że Administratorowi nie wolno już przetwarzać danych w celu objętym sprzeciwem. Nie oznacza to braku możliwości przetwarzania danych w innych celach, o ile Administrator może wskazać inną podstawę prawną przetwarzania.

Po spełnieniu żądania Administrator informuje wnioskodawcę o sposobie realizacji żądania. Informacja powinna być przekazana niezwłocznie, nie później niż w terminie 30 dni od otrzymania żądania. Termin realizacji żądania, w razie potrzeby można przedłużyć o kolejne dwa miesiące, w przypadku kiedy jego realizacja ma skomplikowany charakter. Informację o przedłużeniu terminu realizacji żądania Administrator danych przekazuje wnioskodawcy w terminie 30 dni od złożenia wniosku. Jeżeli wniosek był przekazany w formie elektronicznej, to odpowiedź powinna być również przekazana w takiej formie, chyba że wnioskodawca wskazał inną formę komunikacji.

WYKAZ STOSOWANYCH ZABEZPIECZEŃ

W dokumencie wymieniono stosowane zabezpieczenia techniczne i organizacyjne których celem jest, zgodnie z Art. 32 RODO, zabezpieczenie przetwarzanych danych osobowych przed: przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem oraz nieuprawnionym dostępem do danych osobowych. Poniższy wykaz powinien być aktualizowany każdorazowo, po wdrożeniu nowych zabezpieczeń wynikających między innymi z przeprowadzonej analizy ryzyka.

1. Zabezpieczenia fizyczne

1. Obiekt chroniony jest przez 24 godziny 7 dni w tygodniu przez system połączony z firmą ochroniarską.
2. Dostęp do serwerowni zabezpieczono .....
3. Dostęp do archiwum zabezpieczono drzwiami zamykanymi na klucz.
4. Dostęp do pomieszczeń (w tym biurowych) zabezpieczono drzwiami zamykanymi na klucz.
5. Klucze do pomieszczeń biurowych nadzorowane są i wydawane przez .....
6. W budynku zainstalowany jest system alarmowy na wypadek włamań.
7. Osoby nieupoważnione mogą przebywać w serwerowni wyłącznie w obecności osoby upoważnionej.
8. Rozmieszczono komputery / drukarki / kserokopiarki w sposób ograniczający dostęp do nich osób nieupoważnionych.
9. Dokumenty przechowuje się w zamkniętych niemetalowych i metalowych szafach.

2. Zabezpieczenia techniczne

1. Zastosowano UPS podtrzymujący zasilanie serwerów.
2. W serwerowni zainstalowano czujnik temperatury.
3. Dokumentacja papierowa w archiwum składowana jest na podwyższeniu.

3. Zabezpieczenia organizacyjne

1. Każda osoba, która przetwarza dane osobowe posiada odpowiednie upoważnienie.
2. Ustanowiono politykę haseł.
3. Opracowano procedurę nadawania i zmiany uprawnień do przetwarzania danych osobowych.
4. Opracowano procedurę tworzenia kopii zapasowych i testowego odtwarzania danych z kopii.
5. Opracowano procedurę niszczenia dokumentów i nośników elektronicznych zawierających dane osobowe.
6. Opracowano Regulamin przetwarzania danych osobowych.

4. Zabezpieczenia przed nieautoryzowanym dostępem do sieci lokalnej

1. Dostęp do zasobów sieciowych jest zabezpieczony poprzez zastosowanie autoryzacji wymuszanej przez Active Directory.

2. Zainstalowano oprogramowane antywirusowe na stacjach roboczych.
3. Styk sieci biurowej z Internetem jest chroniony sprzętowo. Zastosowano UTM z aktywną subskrypcją.
4. Wykonuje się aktualizację oprogramowania systemowego zgodnie z zaleceniami producenta.
5. Urządzenia sieciowe konfiguruje się między innymi przez zmianę domyślnych haseł na urządzeniach.
6. W sieci lokalnej stosuje się filtrowanie MAC adresów.
7. Monitoruje się zasoby i obciążenie serwerów.

5. Zabezpieczenia dotyczące infrastruktury IT

1. Zastosowano wirtualizację serwerów.
2. Na stacjach roboczych zastosowano „zahasłowane wygaszacze ekranu", aktywowane po 15 minutach nieaktywności użytkownika.

6. Zabezpieczenia stosowane w aplikacjach

1. Zapewniono rozliczalność operacji dla pracy w aplikacjach. W ramach rozliczalności logowane są operacje tworzenia, zmiany i usuwania rekordu.
2. W celu uzyskania dostępu do aplikacji należy podać informacje uwierzytelniające (login i hasło).

Zał. nr 5 do Polityki

PROCEDURA OBSŁUGI NARUSZEŃ OCHRONY DANYCH OSOBOWYCH

Procedura opisuje sposób zbierania informacji o naruszeniach ochrony danych oraz realizację zadań wynikających z art. 33 i 34 RODO.

Informacje o incydentach i zdarzeniach, które mogą mieć wpływ na bezpieczeństwo danych osobowych mogą wpływać do Administratora danych i IOD, jeżeli został powołany, między innymi z następujących źródeł:
- od pracowników (obowiązek określony w Regulaminie ochrony danych osobowych),
- od ASI (Informatyka),
- z urządzeń monitorujących,
- od podmiotu przetwarzającego.

Każdy zgłoszony incydent i zdarzenie Administrator powinien zweryfikować i stwierdzić czy jest to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Naruszenie ochrony danych to incydent bezpieczeństwa pociągający za sobą skutek w postaci zniszczenia, utraty, nieuprawnionego zmodyfikowania, ujawnienia lub dostępu do danych osób nieuprawnionych. Każde naruszenie ochrony danych powinno być udokumentowane i opisane w Raporcie z naruszenia ochrony danych (zał. nr 5a).

Jeżeli jest mało prawdopodobne, by stwierdzone naruszenie ochrony danych skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych Administrator danych nie ma obowiązku zgłaszać naruszenia organowi nadzorczemu.

W przeciwnym wypadku Administrator danych ma obowiązek bez zbędnej zwłoki, w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, zgłosić je organowi nadzorczemu. Zgłoszenie do organu nadzorczego powinno zawierać informacje opisane w art. 33 ust. 3 RODO. Zgłoszenie do organu nadzorczego powinno powstać w oparciu o Raport z naruszenia ochrony danych. Jeżeli Administratorowi nie uda się dochować 72-godzinnego terminu zgłoszenia o wystąpieniu naruszenia ochrony danych, to musi wyjaśnić przyczyny opóźnienia. Możliwa jest również sytuacja, gdy Administrator przekaże do organu nadzorczego niepełne zgłoszenie, a następnie będzie je sukcesywnie uzupełniał.

Art. 34 RODO nakłada, w niektórych przypadkach, na Administratora obowiązek zawiadomienia osób, których dane dotyczą, o naruszeniu ochrony danych osobowych. Taki obowiązek powstaje, jeżeli naruszenie ochrony danych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

Artykuł 23 ust. 1 RODO przewiduje możliwość wyłączenia w przepisach szczególnych obowiązku informowania osób o naruszeniu ochrony danych. Administrator powinien zatem sprawdzić, czy nie jest wyłączony z takiego obowiązku na mocy obowiązujących go ustaw szczegółowych.

Zawiadomienie osób, których dane dotyczą o naruszeniu ochrony danych nie jest również wymagane, gdy:
- Administrator wdrożył odpowiednie techniczne o organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności szyfrowanie, które uniemożliwia odczyt danych przez osoby nieuprawnione,
- Administrator, po stwierdzeniu naruszenia, zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw i wolności osoby, której dane dotyczą,
- powiadomienie wszystkich osób wymagałoby niewspółmiernego wysiłku – wtedy należy wydać publiczny komunikat o zdarzeniu.

Zawiadomienie osoby, której dane dotyczą o naruszeniu powinno jasnym i prostym językiem opisywać charakter naruszenia ochrony danych osobowych oraz zawierać przynajmniej następujące informacje:
- imię i nazwisko oraz dane kontaktowe IOD lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
- opis możliwych konsekwencji naruszenia ochrony danych osobowych,
- opis środków zastosowanych lub proponowanych przez Administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownym przypadku środków służących zminimalizowaniu ewentualnych negatywnych skutków naruszenia.

Zał. 5a do Polityki

RAPORT
z naruszenia ochrony danych osobowych

w .....

1.Zgłoszenie podejrzenia naruszenia data: ..... godzina: .....

2. Stwierdzenie naruszenia data: ..... godzina: .....

3. Data naruszenia (okres) data: .....

4. Osoba powiadamiająca o zaistniałym zdarzeniu lub źródło informacji:

.....

5. Miejsce naruszenia:

.....

6. Opis naruszenia:

.....
.....

7. Kategoria i ilość osób, których dotyczy naruszenie:

.....
.....

8. Zakres danych lub kategoria danych:

.....
.....

9. Okoliczności naruszenia (opis, analiza zdarzenia, przyczyny wystąpienia):

.....
.....

10. Opis skutków / konsekwencji naruszenia:

.....
.....

11. Podjęte działania naprawcze:

.....
.....

12. Osoba odpowiedzialna za wdrożenie działań naprawczych:

.....
.....

13. Czy zachodzi obowiązek powiadamiania UOD (Tak / Nie): .....

Powiadomienie UOD data ..... godzina .....

14. Czy zachodzi obowiązek poinformowania osób, których naruszenie dotyczy (Tak / Nie) .....
Sposób przekazania informacji:

.....
.....

Opis zaleceń dla podmiotów danych:

.....
.....

.....
(data, podpis ADO)

Zał. nr 6 do Polityki

Poniższa ankieta dotyczy oceny bezpieczeństwa przetwarzania danych osobowych przez podmiot przetwarzający (lub mający przetwarzać po zawarciu odpowiedniej umowy) dane osobowe, powierzane przez .....
Ankieta zawiera pytania, odnoszące się do zabezpieczenia danych osobowych o których mowa w rozporządzeniu Parlamentu Europejskiego i Rady (EU) 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 ogólnym (zwanym dalej RODO).

Lp.	Pytanie	Odpowiedź
1	Czy personel podmiotu przetwarzającego został przeszkolony z zasad przetwarzania danych osobowych, zawartych w RODO?	
2	Czy podmiot przetwarzający wyznaczył osobę, mającą w swoim zakresie obowiązków dbałość o bezpieczeństwo przetwarzania danych osobowych i zarządzanie tym bezpieczeństwem?	
3	Czy do przetwarzania danych są dopuszczane wyłącznie osoby posiadające imienne upoważnienia nadane przez uprawnioną do tego osobę?	
4	Czy osoby, które zostały upoważnione do przetwarzania danych osobowych, zostały równocześnie zobowiązane do zachowania w tajemnicy tych danych oraz sposobów ich zabezpieczenia?	
5	Czy firma opracowała i wdrożyła politykę bezpieczeństwa przetwarzania danych osobowych?	
6	Czy firma posiada wdrożone procedury, umożliwiające bezzwłoczne zgłoszenie Administratorowi naruszenie bezpieczeństwa danych osobowych?	
7	Czy firma stosuje fizyczne zabezpieczenia pomieszczeń w których przetwarzane są dane osobowe przed dostępem osób nieuprawnionych? Jeśli tak, proszę opisać, jakie (np. pomieszczenia zabezpieczone drzwiami zamykanymi na klucz, została wdrożona gospodarka kluczami do pomieszczeń, system kontroli dostępu, systemy antywłamaniowe itp.).	
8	Czy jest stosowane oprogramowanie antywirusowe?	
9	Czy są stosowane środki służące ochronie danych przed ich utratą? Jakie?	
10	Czy jest zapewniona rozliczalność procesów przetwarzania danych osobowych, np. czy istnieje możliwość stwierdzenia kto i kiedy modyfikował dane konkretnej osoby?	
11	Czy umowy lub procedury serwisowe uwzględniają konieczność zapobiegania ujawnieniu chronionych danych osobom niepowołanym, np. w razie konieczności naprawy lub wymiany uszkodzonego sprzętu?	

12	Czy w przypadku przekazywania danych, podlegających ochronie, środkami telekomunikacyjnymi lub na nośnikach wymiennych, ich poufność, integralność i autentyczność jest zabezpieczana metodami kryptograficznymi (np. szyfrowanie)?	
13	Czy są stosowane środki służące ochronie danych przed nieuprawnionym dostępem? Jeśli tak, proszę je zwięźle wymienić: np. identyfikatory i hasła, systemy kontroli dostępu, firewall, itp.	
14	Czy dostęp do systemów operacyjnych komputerów, w których przetwarzane są dane podlegające ochronie, zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz znanego wyłącznie uprawnionemu użytkownikowi hasła? Jeśli tak, to czy zastosowano systemowe mechanizmy wymuszające okresowe zmiany haseł użytkowników?	
15	Czy każda z osób upoważnionych do przetwarzania danych loguje się do systemów, w których przetwarzane są dane osobowe własnym identyfikatorem i hasłem?	
16	Czy zastosowano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych podlegających ochronie?	

Zał. nr 7 do Polityki

Umowa powierzenia przetwarzania danych osobowych (wzór)

zawarta dnia ..... r. pomiędzy:

(zwana dalej „Umową")

....., zwanym w dalszej części umowy **„Podmiotem przetwarzającym"**

a

....., zwaną w dalszej części umowy **„Administratorem danych" lub „Administratorem"**

dalej występujące łącznie jako **„Strony".**

Mając na uwadze, że Strony zawarły umowę ..... , w związku z wykonywaniem której Administrator powierza Podmiotowi przetwarzającemu przetwarzanie danych osobowych Strony postanowiły zawrzeć umowę następującej treści:

§ 1

Powierzenie przetwarzania danych osobowych

1. Administrator danych powierza Podmiotowi przetwarzającemu, w trybie art. 28 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 (Dz.Urz. UE L 119, s. 1), zwanego w dalszej części „Rozporządzeniem", dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.
2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia.

§2

Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał powierzone na podstawie umowy następujące rodzaje danych osobowych: .....

2. Powierzone przez Administratora dane osobowe będą przetwarzane przez podmiot przetwarzający wyłącznie w celu realizacji umowy ..... w zakresie .....

§3

Obowiązki podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanemu z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.
2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim pracownikom, którzy będą przetwarzali powierzone dane.
4. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, (o której mowa w art. 28 ust 3 pkt b Rozporządzenia) przetwarzanych danych przez pracowników, których upoważnia do przetwarzania powierzonych danych, zarówno w trakcie zatrudnienia ich w podmiocie przetwarzającym, jak i po jego ustaniu.
5. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem usuwa wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
6. W miarę możliwości podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.
7. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi w ciągu 72 h.

§4

Prawo kontroli

1. Administrator danych zgodnie z art. 28 ust. 3 pkt h) Rozporządzenia ma prawo kontroli, czy środki zastosowane przez podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.
2. Administrator danych realizować będzie prawo kontroli w godzinach pracy podmiotu przetwarzającego i z minimum 3 dniowym jego uprzedzeniem.
3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych nie dłuższym niż 7 dni.

4. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.

§5

Dalsze powierzenie danych do przetwarzania

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy po uzyskaniu uprzedniej pisemnej zgody Administratora danych.
2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora danych chyba, że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora danych o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Podwykonawca, o którym mowa w §5 ust. 1 Umowy winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na podmiot przetwarzający w niniejszej Umowie.
4. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za nie wywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

§ 6

Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Urząd Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora danych.

§7

Czas obowiązywania umowy

1. Niniejsza umowa obowiązuje od ..... r. na czas obowiązywania Umowy.....

2. Każda ze stron może wypowiedzieć niniejszą umowę z zachowaniem 1 miesięcznego okresu wypowiedzenia.

§8

Rozwiązanie umowy

1. Administrator danych może rozwiązać niniejszą umowę ze skutkiem natychmiastowym gdy podmiot przetwarzający:
   a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
   b) przetwarza dane osobowe w sposób niezgodny z umową;
   c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych.

§9

Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.
2. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy dla Administratora.

_____ _____

Administrator danych Podmiot przetwarzający

Zał. nr 8 do Polityki

Regulamin ochrony danych osobowych obowiązujący w KSM „Nasz dom"

1. Każda osoba dopuszczona do przetwarzania danych osobowych jest zobowiązana do:
   a. przetwarzania danych osobowych wyłącznie w zakresie i celu określonym w upoważnieniu do ich przetwarzania,
   b. zachowania w tajemnicy danych osobowych do których ma dostęp w związku z wykonywaniem obowiązków służbowych,
   c. ochrony danych osobowych przed ich przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem lub przetwarzaniem,
   d. zachowania w tajemnicy sposobów ochrony i zabezpieczania danych.
2. Zabrania się przekazywania bezpośrednio lub przy pomocy środków komunikacji na odległość danych osobowych osobom nieupoważnionym lub osobom których tożsamości nie można zweryfikować.
3. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się podstawą prawną do dostępu do takich danych.
4. Pracownicy są zobowiązani do trwałego zniszczenia dokumentów zawierających dane osobowe przed ich wyrzuceniem.
5. Pracownicy są zobowiązani do zabezpieczania dokumentów oraz nośników przed kradzieżą, wglądem osób nieupoważnionych zarówno podczas ich nieobecności w pomieszczeniu w trakcie godzin pracy jak i po godzinach pracy (np. przez zamykanie w szafach, biurkach, pomieszczeniach).
6. Pracownicy zobowiązani są do szyfrowania plików przechowywanych na nośnikach zewnętrznych (pendrive, dyski zewnętrzne), jeżeli w plikach przechowywane są dane osobowe.
7. Zabrania się zostawiania otwartych pomieszczeń, w których przetwarza się dane osobowe zarówno w godzinach pracy jak i po jej zakończeniu.
8. Każdorazowo przed opuszczeniem stanowiska pracy pracownik zobowiązany jest do zablokowania komputera przez użycie skrótu klawiszowego Windows +L.
9. Pracownicy zobowiązani są do stosowania zasady czystego biurka i czystego ekranu.

Zasady pracy w systemach informatycznych

1. Zabrania się pracy wielu pracowników na wspólnym identyfikatorze.
2. Każdy pracownik zobowiązany jest do posługiwania się własnym loginem (identyfikatorem) i hasłem w celu uzyskania dostępu do systemu informatycznego.
3. Zabrania się ujawniania loginu i hasła współpracownikom i osobom z zewnątrz.
4. Zabrania się pracy w systemach informatycznych z wykorzystaniem cudzego loginu.
5. Pracownicy, którzy usiłują uzyskać dostęp do chronionych zasobów w sposób nielegalny, naruszają niniejszy regulamin i narażają się na odpowiedzialność służbową i karną.
6. Każdy pracownik zobowiązany jest do stosowania polityki haseł obowiązującej u Administratora, która wymaga między innymi, by:
   a. hasło zawierało co najmniej 14 znaków,
   b. hasło nie znajdowało się w słowniku słabych / często używanych haseł publikowanych przez CERT Polska,
   c. stosowane hasła były trudne do odgadnięcia,
   d. haseł nie ujawniać innym osobom,
   e. hasła przechowywać w miejscach niedostępnych dla innych osób.
10. Zabrania się Pracownikom:
    a. samodzielnej naprawy, przeróbki, rozbudowy lub ingerencji w konfigurację sprzętu komputerowego oraz systemów informatycznych,
    b. instalowania lub usuwania oprogramowania bez konsultacji z Administratorem lub Administratorem Systemów Informatycznych,
    c. wykorzystywania sieci do nielegalnego ściągania materiałów chronionych prawem autorskim, oraz przechowywania w zasobach informatycznych organizacji takich materiałów,

d. przesyłania danych i dokumentów służbowych przez komunikatory internetowe, sieci p2p oraz do prywatnych chmur (np. dyski goole) i na adres prywatnej poczty elektronicznej,
e. podłączania do gniazdek przeznaczonych do zasilania komputerów urządzeń o dużym poborze mocy, takich jak: czajniki elektryczne, grzejniki itp.,
f. usuwania lub przerabiania oznaczeń z numerami inwentarzowymi, licencyjnymi lub innymi, którymi sprzęt został oznaczony,
g. zmiany lokalizacji sprzętu komputerowego bez uzgodnienia z Administratorem Systemu Informatycznego.
h. Zabrania się wyłączania lub zmiany konfiguracji systemu antywirusowego zainstalowanego na komputerze.
i. Zabrania się przechowywania niezabezpieczonych plików, które zawierają dane osobowe, na komputerach wykorzystywanych przez grupę pracowników.

Zasady korzystania z poczty elektronicznej

1. Dane osobowe przesyłane za pomocą poczty elektronicznej powinny być odpowiednio zabezpieczone (zaszyfrowane lub zabezpieczone hasłem), a hasło nie powinno być wysłane w tym samym mailu.
2. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW".
3. Użytkownicy powinni okresowo kasować maile. Dotyczy to zwłaszcza maili zawierających dane osobowe.
4. Mail służbowy jest przeznaczony do wykonywania obowiązków służbowych.
5. Zabrania się otwierania załączników (.xlsm, .exe) w mailach od nieznanych nadawców. Są to ~~zwykle~~ „wirusy", które mogą zainfekować komputer.
6. Zabrania się „klikać" na hiperlinki w mailach od nieznanych nadawców, gdyż mogą to być hiperlinki do stron z „wirusami".
7. Zabrania się użytkownikom poczty elektronicznej konfigurowania swoich kont pocztowych do automatycznego przekierowywania wiadomości na adres zewnętrzny.

Zasady korzystania z internetu

1. Pracownicy mogą korzystać z internetu wyłącznie w celach służbowych.
2. Zabrania się korzystania w trakcie pracy z serwisów ewidentnie nie związanych z zakresem wykonywanych obowiązków służbowych (np. serwisy randkowe, udostępniające treści zakazane prawem lub treści chronione prawem autorskim).
3. Zabrania się włączania w opcjach przeglądarki internetowej zapamiętywania haseł.

Obowiązek zgłaszania podatności i incydentów zagrażających bezpieczeństwu danych osobowych

1. Pracownicy zobowiązani są do powiadomienia zwierzchnika i IOD o podatnościach i incydentach, które mogą zagrażać bezpieczeństwu danych osobowych.
2. Do podatności, które wymagają powiadomienia, należą:
    a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
    b. niewłaściwe zabezpieczenie sprzętu IT i oprogramowania przed wyciekiem, kradzieżą lub utratą danych osobowych.
3. Do incydentów wymagających powiadomienia, należą:
    a. zdarzenia losowe zewnętrzne (pożar, zalanie wodą),
    b. zdarzenia losowe wewnętrzne (awarie serwerów, twardych dysków, utrata / zagubienie danych)
    c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych).
4. Typowe przykłady incydentów wymagające reakcji:
    a. ślady na drzwiach, oknach i szafach wskazujące na próbę włamania,
    b. niewłaściwy sposób niszczenia dokumentacji,
    c. ustawienie monitorów pozwalające na wgląd osób postronnych w dane osobowe,
    d. ujawnienie osobom nieuprawnionym danych osobowych,
    e. telefoniczne próby wyłudzenia danych osobowych,
    f. kradzież, zagubienie komputerów lub nośników zawierających dane osobowe,
    g. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów,

h. rażące naruszenie obowiązków w zakresie przestrzegania procedur bezpieczeństwa informacji (pozostawienie danych w drukarce lub kserokopiarce, niewykonanie kopii zapasowych, prace na danych osobowych w celach prywatnych itp.);

Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego regulaminu są naruszeniem obowiązków pracowniczych i mogą stanowić podstawę do nałożenia kary dyscyplinarnej.

Załącznik Nr 2 do uchwały nr 29/2026
Zarządu KSM „Nasz Dom" w Koszalinie
z dnia 26 maja 2026 roku

Koszalińska Spółdzielnia Mieszkaniowa „NASZ DOM" w Koszalinie

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

Zatwierdził:

ZASTĘPCA PREZESA ZARZĄDU
ds. ekonomiczno-finansowych
GŁÓWNY KSIĘGOWY
26.05.2026r.
mgr Ewelina Kowalska
(data, podpis)

PREZES ZARZĄDU
KSM „Nasz Dom"
mgr inż. Jacek Janczewski

Niniejsza Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej Instrukcją, przyjęta została w celu wykazania, że dane osobowe w systemach informatycznych wykorzystywanych przez KSM „NASZ DOM" przetwarzane są w sposób zgodny z przepisami prawa mającymi zastosowanie do takiej czynności, zgodnie z zasadą art. 5 ust. 1 lit. f) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej RODO).

I. Procedura nadawania, zmiany i odbierania uprawnień

Celem procedury jest minimalizacja ryzyka przetwarzania danych przez osoby nieupoważnione i ich ujawnienia z powodu braku świadomości konieczności ochrony danych osobowych.

1. Jednym z etapów procesu zatrudnienia nowego pracownika, który będzie przetwarzał dane osobowe, jest przesłanie przez Specjalistę ds. Kadr do IOD następujących informacji:
   - imię i nazwisko pracownika,
   - stanowisko,
   - służbowy adres email (do przesłania linku do szkolenia i testu).
2. Każdy pracownik przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z:
   - zasadami przetwarzania i ochrony danych osobowych zawartych w Rozporządzeniu 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 (RODO),
   - dokumentacją wewnętrzną dotyczącą ochrony danych osobowych,
   - Regulaminem ochrony danych osobowych.

   Szkolenie odbywa się w formie nagranego wykładu. Zaliczenie szkolenia następuje przez przesłanie na wskazany w mailu adres odpowiedzi na załączony test.
3. Po zaliczeniu szkolenia i podpisaniu oświadczenia o zachowaniu poufności (zał. nr 1 do Instrukcji) IOD wystawia upoważnienie do przetwarzania danych osobowych l (zał. nr 2 do Instrukcji) i aktualizuje wykaz osób uprawnionych do przetwarzania danych osobowych. Upoważnienie do przetwarzania danych osobowych zatwierdza Prezes lub upoważniona przez niego pisemnie osoba.
4. Dla każdego pracownika nadawany jest indywidualny identyfikator (login), który umożliwia dostęp do stacji roboczej, zasobów sieciowych i aplikacji. Identyfikator użytkownika po wyrejestrowaniu z systemu informatycznego nie może być przydzielony innej osobie.
5. Nadawanie, zmiana i odbieranie dostępów odbywa się na polecenie bezpośredniego przełożonego i jest realizowane przez Administratora Systemu Informatycznego (w przypadku systemów przetwarzanych na wewnętrznym serwerze) lub wskazaną osobę (w przypadku systemów zewnętrznych).
6. Podstawę do nadania uprawnień stanowi Karta przydziału zasobów (zał. nr 3 do Instrukcji).
7. W przypadku zmiany zakresu przydzielonych obowiązków administrator odpowiednio modyfikuje uprawnienia do pracy w aplikacjach dziedzinowych.

8. Przy przydzielaniu uprawnień obowiązuje zasada minimalizacji uprawnień.
9. Użytkowników obowiązuje zasada pracy z użyciem własnego loginu. Zabroniona jest praca w jakimkolwiek elemencie systemu informatycznego na loginie innego użytkownika.
10. W przypadku zwolnienia pracownika do Karty obiegowej dodawana jest Karta przydziału zasobów, która stanowi podstawę odebrania uprawnień w systemach przetwarzanych na serwerach organizacji i w systemach zewnętrznych.
11. Informację o zwolnieniu pracownika Specjalista ds. Kadr przekazuje do IOD w celu aktualizacji Rejestru osób upoważnionych do przetwarzania danych osobowych.

II. Polityka haseł (metody i środki uwierzytelniania)

Stosowanie polityki haseł zapewnia, że do systemów informatycznych, w których są przetwarzane dane osobowe mają dostęp tylko osoby do tego upoważnione.
Administrator stosuje następujące wymogi w stosunku do budowy hasła, jego użytkowania i przechowywania:

1. Użytkownik komputera i aplikacji, w celu uwierzytelnienia podaje indywidualny login i hasło.
2. Hasło użytkownika powinno mieć minimum 14 znaków.
3. Nowe hasło jest weryfikowane, czy nie znajduje się w słowniku słabych/często używanych haseł publikowanych przez CERT Polska.
4. Hasła wpisywane z klawiatury nie mogą pojawiać się na ekranie monitorów w formie jawnej.
5. Hasło nie może być zapisywane w miejscu dostępnym dla osób nieuprawnionych.
6. Użytkownik nie może udostępnić swojego identyfikatora oraz hasła jak również dostępu do stanowiska roboczego po uwierzytelnieniu w systemie osobom nieuprawnionym.
7. Hasło użytkownika należy utrzymywać w tajemnicy, również po upływie jego ważności.
8. W przypadku, gdy istnieje podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik zobowiązany jest do natychmiastowej zmiany hasła, lub w razie problemów do powiadomienia o tym fakcie Administratora Systemu Informatycznego.
9. Aktualne hasła administracyjne do systemów, aplikacji, urządzeń przechowywane są w dwóch lokalizacjach dostępnych dla Administratora Systemu Informatycznego oraz u Głównej Księgowej KSM „NASZ DOM".
10. W przypadkach awaryjnych, przy nieobecności Administratora Systemu Informatycznego, hasło może być przekazane decyzją Prezesa innej osobie.
11. Po ustaniu sytuacji awaryjnej Administrator Systemu Informatycznego jest zobowiązany do zmiany ujawnionego hasła.
12. W przypadku utraty uprawnień przez Administratora Systemu Informatycznego należy niezwłocznie zmienić wszystkie hasła, do których miał on dostęp.

III. Kopie zapasowe

Celem procedury jest zapewnienie, że w przypadku awarii serwera lub stacji roboczej oraz zakłócenia spójności lub dostępności danych z różnych powodów istnieje możliwość ich odtworzenia.

1. Kopia zapasowa danych przetwarzanych w systemie MIESZCZANIN wykonywana jest w trybie codziennym na dysk serwera, raz w tygodniu na urządzenie NAS i raz w miesiącu na dysk zewnętrzny, który jest przechowywany we wskazanym miejscu u Administratora.
2. Kopia obrazu systemu wykonywana jest raz w tygodniu na urządzenie NAS.
3. W trybie codziennym wykonywane są kopie danych przechowywanych na pulpicie, w katalogu „Moje dokumenty" oraz z outlooka ze wszystkich stacji roboczych. Raz w tygodniu kopia tych danych wykonywana jest również na urządzenie NAS.
4. Za wykonywanie w/w kopii odpowiada Administrator Systemu Informatycznego.
5. Zabrania się wykonywania „prywatnych kopii danych" na nośnikach zewnętrznych i w chmurach obliczeniowych.
6. Administrator Systemu Informatycznego, w celu weryfikacji poprawności, okresowo odtwarza dane z kopii zapasowych.

IV. Procedura niszczenia nośników elektronicznych i dokumentów papierowych

Celem procedury jest zapewnienie, że osoby nieupoważnione nie będą miały dostępu do informacji zapisanych na nośnikach elektronicznych i w dokumentach papierowych, które utraciły swą przydatność.

1. Każdorazowo przed wycofaniem komputera z eksploatacji lub przeniesieniem na inne stanowisko należy przekazać go Informatykowi, by ten we właściwy sposób usunął informacje zapisane na dysku.
2. W przypadku konieczności przekazania komputera do naprawy, o ile to możliwe należy wyciągnąć z niego dysk twardy. Jeżeli nie ma takiej możliwości, to naprawa odbywa się w siedzibie Administratora danych.
3. Elektroniczne nośniki informacji (dyski twarde z komputerów i serwerów, pendrive), które nie będą już wykorzystywane z powodu uszkodzenia lub utraty możliwości ich wykorzystania składowane są w wyznaczonym, chronionym miejscu.
4. Okresowo wszystkie nośniki elektroniczne są komisyjnie niszczone w sposób fizyczny lub poprzez demagnetyzację.
5. Zniszczenie nośników jest potwierdzone protokołem zniszczenia podpisanym przez osoby uczestniczące w niszczeniu.
6. Doraźnie dokumentacja papierowa niszczona jest w niszczarkach.
7. W przypadku konieczności zniszczenia dużych ilości dokumentacji papierowej jest ona przekazywana do firmy niszczącej dokumenty papierowe. Firma wystawia certyfikat potwierdzający zniszczenie dokumentów. Z firmą tą należy podpisać umowę powierzenia przetwarzania danych osobowych.

V. Procedura bezpiecznego korzystania z komputerów przenośnych

Celem procedury jest wskazanie podstawowych zabezpieczeń informatycznych i fizycznych, które powinny być stosowane przy konfiguracji komputera oraz podczas jego użytkowania.

1. Dysk komputera przenośnego powinien być zabezpieczony hasłem.
2. Hasło do dysku komputera jest przechowywane u Administratora Systemu Informatycznego.
3. Komputera przenośnego nie należy pozostawiać bez nadzoru w miejscach publicznych, między innymi w samochodzie czy przechowalni bagażu.
4. Z komputera przenośnego należy korzystać w sposób minimalizujący ryzyko dostępu do przetwarzanych danych przez osoby nieupoważnione.
5. Przy korzystaniu z komputera przenośnego w miejscach publicznych i w środkach transportu publicznego należy chronić informacje wyświetlane na monitorze przed wglądem osób nieuprawnionych.
6. Zabrania się dopuszczania osób nieupoważnionych do korzystania z komputera przenośnego na którym przetwarzane są dane osobowe.
7. W przypadku kradzieży lub zagubienia komputera przenośnego należy bezzwłocznie powiadomić Administratora Danych.

Zał. nr 1 do Instrukcji

OŚWIADCZENIE
O ZACHOWANIU POUFNOŚCI

Ja niżej podpisany(-a) .....

zatrudniony(-a) w Koszalińskiej Spółdzielni Mieszkaniowej „NASZ DOM" zostałem(-am) zapoznany(-a) z przepisami:

1. Rozporządzeniem Parlamentu Europejskiego i Rady 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,
2. Polityką ochrony danych osobowych.

Niniejszym zobowiązuję się do:
- przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Administratora zadaniach,
- przestrzegania zasad wynikających z powszechnie obowiązujących przepisów prawa oraz regulacji wewnętrznych dotyczących ochrony danych osobowych, w tym Regulaminu ochrony danych osobowych,
- zachowania w tajemnicy danych osobowych, do których mam lub będę miał(-a) dostęp w związku z wykonywaniem obowiązków wynikających ze stosunku zatrudnienia, zarówno w trakcie jego trwania, jak i po ustaniu,
- zachowania w tajemnicy sposobów zabezpieczania danych osobowych,
- ochrony danych osobowych przed ich przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem do nich.

Oświadczam, że zostałam(-em) pouczona(-y) o odpowiedzialności za niedopełnienie obowiązków wynikających z niniejszego oświadczenia.

Czytelny podpis składającego
Data oświadczenie

....

Załącznik nr 2 do Instrukcji

Koszalin, dn. .....

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 (Dz.Urz. UE L 119, s. 1) – dalej **RODO** – nadaję upoważnienie Pani/Panu:

.....

zatrudnionej(-mu) na stanowisku .....

do przetwarzania danych osobowych w zakresie niezbędnym do wykonywania obowiązków na ww. stanowisku.

Upoważnienie obowiązuje na czas zajmowania w/w stanowiska.

Zobowiązuję Panią/Pana do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem oraz z przepisami RODO i ustawami szczegółowymi a także z wewnętrznymi regulacjami dotyczącymi przetwarzania danych osobowych u Pracodawcy.

Jednocześnie upoważniam 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 u Pracodawcy.

.....

podpis osoby uprawnionej do nadania poważnienia

Zapoznałam / zapoznałem się z treścią upoważnienia

.....

podpis osoby przyjmującej upoważnienie

Załącznik nr 3 do Instrukcji

Karta przydziału zasobów

Imię i nazwisko pracownika .....

Identyfikator .....

Przydział zasobów w sieci:

Zasób	**Nazwa systemu / modułu**	**Informacja o przydziale zasobu** (T-tak; N-nie)	**Przydział dostępu do zasobu** (Data i podpis administratora)	**Odebranie dostępu do zasobu** (Data i podpis administratora)
Konto w domenie				
Zdalny dostęp do zasobów sieciowych (VPN)				
Skrzynka pocztowa				
System MIESZCZANIN	E-kartoteka			
	System Łatwej Obsługi Nieruchomości			
	Finanse i Księgowość			
	Techniczna Obsługa Nieruchomości			
	Banki			
	Kadry i Płace			
	Nieruchomości – Członkowie - Wkłady			
	Fakturowanie			
	Środki Trwałe			
	Kasa			
	Centrala			
	Magazyn			

Systemy zewnętrzne:

Nazwa systemu	**Administrator**	**Informacja o przydziale dostępu** (T-tak; N-nie)	**Przydział dostępu do zasobu** (Data i podpis administratora)	**Odebranie dostępu do zasobu** (Data i podpis administratora)
ZU-MA				
TECHEM				
MINOL				
PUE ZUS				
Płatnik				

.....

Data i podpis Przełożonego