

Zarządzenie nr 4/2025
Prezesa Zarządu
Międzyzakładowej Spółdzielni Mieszkaniowej „Chemik” w Płocku
z dnia 24 stycznia 2025 roku

w sprawie wprowadzenia Polityki Bezpieczeństwa Danych Osobowych
w MSM „Chemik”

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 (ogólne rozporządzenie o ochronie danych) zarządza się, co następuje:

§ 1.

Z dniem 24 stycznia 2025 roku wprowadza się Politykę Bezpieczeństwa Danych Osobowych w Międzyzakładowej Spółdzielni Mieszkaniowej „Chemik” w Płocku.

§ 2.

Polityka Bezpieczeństwa Danych Osobowych w MSM „Chemik” stanowi załącznik do niniejszego zarządzenia.

§ 3.

Z dniem wejścia w życie niniejszego zarządzenia, traci moc Zarządzenie nr 9/2006 Prezesa Zarządu MSM „Chemik” z dnia 01.09.2006 r. w sprawie ochrony danych osobowych, zmienione Aneksem nr 1/2017 z dnia 23.02.2017 r.

§ 4.

Zarządzenie wchodzi w życie z dniem 24 stycznia 2025 roku.

PREZES ZARZĄDU
Międzyzakładowej Spółdzielni Mieszkaniowej
„Chemik” w Płocku

Piotr Gwóźdź

Załącznik nr 1 do Zarządzenia nr 4/2025
Prezesa Zarządu MSM „Chemik”
z dnia 24.01.2025 r.

**POLITYKA BEZPIECZEŃSTWA
DANYCH OSOBOWYCH
MIĘDZYZAKŁADOWEJ SPÓŁDZIELNI
MIESZKANIOWEJ „CHEMIK”
W PŁOCKU**

Wymagania prawne:	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).
--------------------------	---

SPIS TREŚCI:

1. Wykaz podstawowych skrótów	3
2. Wykaz podstawowych definicji	3
3. Wprowadzenie	4
4. Cele Polityki Bezpieczeństwa Danych Osobowych	5
5. Zakres rozpowszechniania Polityki Bezpieczeństwa Danych Osobowych	5
6. Inspektor Ochrony Danych	5
7. Osoby upoważnione do przetwarzania danych osobowych	5
8. Podstawowe zasady ochrony danych osobowych	6
9. Upoważnienie do przetwarzania danych osobowych	6
10. Powierzenie przetwarzania danych osobowych	7
11. Udostępnianie danych osobowych	7
12. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe	7
13. Opis struktury zbiorów danych osobowych	7
14. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych	8
15. Przepisy karne i porządkowe	8
16. Postanowienia końcowe	8

1. Wykaz podstawowych skrótów

Skrót	Opis
ADO	Administrator Danych Osobowych
IOD	Inspektor Ochrony Danych
MSM „Chemik”	Międzyzakładowa Spółdzielnia Mieszkaniowa „Chemik” w Płocku
SI	System Informatyczny
PBDO	Polityka Bezpieczeństwa Danych Osobowych
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)

2. Wykaz podstawowych definicji

Ilekcroć w niniejszej Polityce Bezpieczeństwa Danych Osobowych mowa o:

Administratorze Danych Osobowych – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;

Administratorze Systemu Informatycznego – rozumie się przez to pracownika Administratora Danych Osobowych lub inne osoby odpowiedzialne za funkcjonowanie systemów i sieci teleinformatycznych oraz za przestrzeganie zasad i wymogów bezpieczeństwa systemów i sieci teleinformatycznych;

Inspektorze Ochrony Danych – rozumie się przez to osobę odpowiedzialną za bieżący nadzór stosowania przepisów dot. ochrony danych osobowych;

Osobie upoważnionej – rozumie się przez to osobę upoważnioną przez Administratora Danych Osobowych do przetwarzania danych osobowych. Osobą upoważnioną może być pracownik Spółki, osoba wykonująca prace na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, a także osoba odbywająca wolontariat, praktykę lub staż;

Danych osobowych – rozumie się przez to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”);

Możliwej do zidentyfikowania osobie fizycznej - rozumie się przez to 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;

Przetwarzaniu danych osobowych – rozumie się przez to operację 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;

Zbiorze danych osobowych – rozumie się przez to uporządkowany zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

- Podmiocie przetwarzającym** – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora Danych Osobowych;
- Odbiorcy danych** - rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;
- Systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;
- Bezpieczeństwie danych osobowych** – rozumie się przez to zespół zasad, jakimi należy się kierować projektując oraz wykorzystując systemy i aplikacje służące do przetwarzania danych osobowych, by w każdych okolicznościach dostęp do nich był zgodny z założeniami i zapewniał ich poufność, integralność oraz dostępność;
- Poufności danych** – rozumie się przez to właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym osobom lub podmiotom;
- Integralności danych** – rozumie się przez to właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
- Dostępności danych** – rozumie się przez to właściwość zapewniająca, że dane są osiągalne i możliwe do wykorzystania na żądanie, w założonym czasie, przez uprawnioną osobę lub podmiot;
- Zgodzie osoby, której dane dotyczą** – rozumie się przez to dobrowolne, konkretne, świadome i jednoznaczne okazanie woli przez osobę, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwalające na przetwarzanie dotyczących jej danych osobowych;
- Państwie trzecim** – rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego;
- Incydencie** – rozumie się przez to naruszenie bezpieczeństwa danych osobowych;
- Zagrożeniu** - rozumie się przez to potencjalną możliwość wystąpienia incydentu;
- Naruszeniu ochrony danych osobowych** - rozumie się przez to naruszenie bezpieczeństwa danych osobowych 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.

3. Wprowadzenie

Polityka Bezpieczeństwa Danych Osobowych określa reguły przetwarzania danych osobowych oraz sposobów ich zabezpieczenia, jako zestaw praw, zasad i zaleceń regulujących sposób ich zarządzania, ochrony i dystrybucji w Międzyzakładowej Spółdzielni Mieszkaniowej „Chemik” w Płocku.

Polityka zawiera informacje dotyczące rozpoznawania procesów przetwarzania danych osobowych oraz wprowadzonych zabezpieczeń techniczno-organizacyjnych, zapewniających ochronę przetwarzanych danych osobowych. Niniejszy dokument jest zgodny z obowiązującymi przepisami prawa, a w szczególności z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

4. Cele Polityki Bezpieczeństwa Danych Osobowych

Celem Polityki Bezpieczeństwa Danych Osobowych jest określenie oraz wdrożenie zasad bezpieczeństwa i ochrony danych osobowych przetwarzanych w MSM „Chemik” w szczególności:

- 1) zapewnienie spełnienia wymagań prawnych;
- 2) zapewnienie poufności, integralności oraz rozliczalności danych osobowych przetwarzanych w firmie;
- 3) podnoszenie świadomości osób przetwarzających dane osobowe;
- 4) zaangażowanie osób przetwarzających dane osobowe firmy w ich ochronę.

5. Zakres rozpowszechniania Polityki Bezpieczeństwa Danych Osobowych

1) Z treścią niniejszej Polityki Bezpieczeństwa Danych Osobowych powinny zapoznać się wszystkie podmioty przetwarzające dane osobowe w imieniu Administratora Danych Osobowych.

6. Inspektor Ochrony Danych

- 1) **Inspektor Ochrony Danych** monitoruje przestrzeganie zasad bezpieczeństwa oraz prowadzi kontrolę przetwarzania danych osobowych.
- 2) **Inspektor Ochrony Danych** wykonuje w szczególności następujące zadania:
 - a) zapewnienia przestrzeganie przepisów o ochronie danych osobowych, w szczególności poprzez informowanie, kontrolę i nadzór nad wszelkimi działaniami MSM „Chemik” w zakresie PBDO
 - b) opiniowanie, pod względem zgodności z PBDO oraz z przepisami prawa umów, procedur i innych wytworzonych dokumentów dotyczących bezpieczeństwa i przetwarzania danych osobowych;
 - c) podejmowanie lub wnioskowanie o podjęcie odpowiednich działań w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa danych osobowych oraz prowadzenie adekwatnej dokumentacji w tym zakresie;
- 3) **Inspektor Ochrony Danych** uprawniony jest do:
 - a) kontrolowania stosowania PBDO przez wszystkie działy organizacyjne MSM „Chemik” przy wykonywaniu prac bieżących
 - b) wglądu do dokumentacji organizacyjnej MSM „Chemik” w celu weryfikacji przestrzegania PBDO
 - c) uczestniczenia podczas realizowania zadań bieżących pracowników MSM „Chemik” w celu weryfikacji przestrzegania procedurach PBDO
- 4) **Inspektor Ochrony Danych** może wykonywać swoje obowiązki poprzez wyznaczonych zastępców.
- 5) **Administrator Danych Osobowych** upoważnia **Inspektora Ochrony Danych** do przetwarzania danych osobowych we wszystkich zbiorach **Administratora Danych Osobowych** oraz poza nimi w zakresie niezbędnym dla należytego wykonywania funkcji **Inspektora Ochrony Danych**, a także do wydawania w imieniu **Administratora Danych Osobowych** upoważnień do przetwarzania danych osobowych.

7. Osoby upoważnione do przetwarzania danych osobowych

- 1) Do obowiązków osób upoważnionych do przetwarzania danych osobowych należy:
 - zapoznanie się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami Polityki Bezpieczeństwa Danych Osobowych;
 - stosowanie się do zaleceń Inspektora Ochrony Danych;
 - przetwarzania danych osobowych wyłącznie w zakresie ustalonym indywidualnie przez

Administradora Danych Osobowych w pisemnym upoważnieniu i tylko w celu wykonywania nałożonych obowiązków służbowych;

- niezwłoczne informowanie Inspektora Ochrony Danych o wszelkich nieprawidłowościach dotyczących bezpieczeństwa danych osobowych przetwarzanych w firmie;
- ochronę danych osobowych oraz środków wykorzystywanych do przetwarzania danych osobowych przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem;
- korzystanie z systemów informatycznych firmy w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemów informatycznych;
- bezterminowe zachowanie w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia;
- zachowanie szczególnej staranności w trakcie wykonywania operacji przetwarzania danych osobowych w celu ochrony interesów osób, których dane dotyczą.

8. Podstawowe zasady ochrony danych osobowych

- 1) Wszystkie dane osobowe w firmie należy przetwarzać zgodnie z obowiązującymi przepisami prawa.
- 2) W stosunku do osób, których dane osobowe są przetwarzane należy spełnić obowiązek informacyjny wynikający z przepisów RODO.
- 3) Zebrane dane osobowe należy przetwarzać dla oznaczonych i zgodnych z prawem celów i nie poddawać dalszemu przetwarzaniu niezgodnemu z tymi celami.
- 4) Należy zadbać, aby przetwarzanie danych osobowych odbywało się zgodnie z zasadami dotyczącej merytorycznej poprawności oraz adekwatnie do celów w jakich zostały zebrane.
- 5) Dane osobowe w firmie można przetwarzać nie dłużej niż jest to niezbędne do osiągnięcia celu ich przetwarzania.
- 6) Należy zapewnić poufność, integralność oraz rozliczalność danych osobowych przetwarzanych w firmie.
- 7) Przetwarzane dane osobowe nie mogą być udostępniane bez zgody osób, których dane dotyczą, chyba że udostępnia się te dane osobom, których dane dotyczą, osobom upoważnionym do przetwarzania danych osobowych, podmiotom którym przekazano dane na podstawie umowy powierzenia oraz organom państwowym lub organom samorządu terytorialnego w związku z prowadzonym postępowaniem.
- 8) Przetwarzanie danych osobowych w firmie może odbywać się zarówno w systemach informatycznych, jak i w formie tradycyjnej: kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych.
- 9) W zakresie danych osobowych przetwarzanych w innych systemach niż informatyczne, obowiązują nadal dotychczasowe przepisy o tajemnicy służbowej, obiegu i zabezpieczaniu dokumentów służbowych.
- 10) Wszystkim osobom, których dane są przetwarzane przysługuje prawo do ochrony danych ich dotyczących, do kontroli przetwarzania tych danych oraz do ich uaktualniania, usunięcia jak również do uzyskiwania wszystkich informacji o przysługujących im prawach.

9. Upoważnienie do przetwarzania danych osobowych

- 1) Do przetwarzania danych osobowych i obsługi zbiorów informatycznych zawierających te dane mogą być dopuszczone wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych przez Administratora Danych Osobowych oraz złożyły stosowne oświadczenie dot. właściwej

realizacji przepisów RODO.

- 2) Administrator Danych Osobowych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych.

10. Powierzenie przetwarzania danych osobowych

- 1) Administrator Danych Osobowych może zlecić innemu podmiotowi przetwarzanie danych osobowych w celu realizacji określonego zadania.
- 2) W sytuacji powierzenia przetwarzania danych osobowych podmiotowi zewnętrznemu, w umowie powierzenia przetwarzania danych osobowych określa się przede wszystkim przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.

11. Udostępnianie danych osobowych

- 1) Dane osobowe udostępnia się na wniosek zgodnie z PBDO.
- 2) Wniosek o udostępnienie danych, który wpłynął do firmy rozpatruje ADO.
- 3) Wniosek o udostępnienie danych osobowych, którego sposób rozpatrzenia budzi uzasadnione wątpliwości, może zostać przesłany, wraz z informacjami niezbędnymi dla jego rozpatrzenia, do Inspektora Ochrony Danych w celu zajęcia stanowiska w sprawie. Do wniosku dołącza się projekt odpowiedzi wraz z uzasadnieniem.
- 4) Informacje, zawierające dane osobowe są udostępniane uprawnionym podmiotom:
 - a) w formie wydruku listem poleconym lub za potwierdzeniem osobistego odbioru,
 - b) w drodze teletransmisji danych (w sposób gwarantujący poufność przesyłanych danych),
 - c) na elektronicznych nośnikach informacji, za potwierdzeniem odbioru,
 - d) w inny sposób określony przepisami prawa lub umową.
- 5) Udostępniane dane osobowe podlegają kontroli przez Inspektora Ochrony Danych Osobowych.
- 6) Ewidencja przypadków udostępnienia danych prowadzona jest przez AOD w wersji elektronicznej lub papierowej.
- 7) Ewidencja udostępnień prowadzona jest w wersji elektronicznej lub papierowej.
- 8) AOD zobowiązany jest umożliwić dostęp Inspektorowi Ochrony Danych do prowadzonych ewidencji udostępnień.

12. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

Inspektor Ochrony Danych jest za prowadzenie i przechowywanie dokumentacji zawierającej wykaz budynków, pomieszczeń lub części pomieszczeń tworzący obszar, w którym przetwarzane są dane osobowe zarówno w formie papierowej jak i elektronicznej.

13. Opis struktury zbiorów danych osobowych

Inspektor Ochrony Danych odpowiedzialny jest za prowadzenie i przechowywanie dokumentacji zawierającej opis struktury zbiorów danych osobowych przetwarzanych w firmie.

14. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

Inspektor Ochrony Danych odpowiedzialny jest za prowadzenie i przechowywanie dokumentacji zawierającej określone środki techniczne i organizacyjne niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

15. Przepisy karne i porządkowe

Przepisy karne i porządkowe reguluje:

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).

16. Postanowienia końcowe

W sprawach nieuregulowanych w niniejszej Polityce Bezpieczeństwa Danych Osobowych mają zastosowanie przepisy 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).


PREZES Zarządu
Międzyzakładowej Spółdzielni Mieszkaniowej
„ChemiK” w Ploeku
Piotr Gwóźdź