POLITYKA BEZPIECZEŃSTWA

Administrator Danych Osobowych - CUIAVIA Okręgowa Spółdzielnia Mleczarska siedzibą w Inowrocławiu (88-100) przy ul. Nowej 32, wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy w Bydgoszczy, XIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod nr KRS 0000024724, NIP 556-080-14-07, REGON 000437346

wdraża dokument o nazwie „Polityka Bezpieczeństwa". Zapisy tego dokumentu wchodzą w życie z dniem 25 maja 2018 r.

Polityka ta zgodna jest z postanowieniami:

Konstytucji Rzeczypospolitej Polski

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 (ogólne rozporządzenie o ochronie danych)

Ustawy o ochronie danych osobowych z dnia 10 maja 2018 r.

§ 1.

Polityka bezpieczeństwa w zakresie ochrony danych osobowych w Cuiavii Okręgowej Spółdzielni Mleczarskiej w Inowrocławiu, określa zasady przetwarzania danych osobowych oraz środki techniczne i organizacyjne zastosowane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.
Polityka bezpieczeństwa służy zapewnieniu wysokiego poziomu bezpieczeństwa przetwarzanych danych.
Polityka bezpieczeństwa dotyczy danych osobowych przetwarzanych w zbiorach manualnych oraz w systemach informatycznych.

§ 2

Ilekroć w „Polityce Bezpieczeństwa" jest mowa o:

1. zbiorze danych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
2. przetwarzaniu danych - rozumie się przez to jakiekolwiek operacje lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany takie jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie, lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie ograniczanie usuwanie lub niszczenie,
3. systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
4. zabezpieczeniu danych w systemie informatycznym - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
5. usuwaniu danych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie identyfikację tożsamości osoby, której dane

dotyczą,

6. naruszenie ochrony danych osobowych - oznacza 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
7. administratorze danych - rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, która samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych,
8. podmiocie – rozumie się przez to spółkę prawa handlowego, podmiot gospodarczy nie posiadający osobowości prawnej, jednostkę budżetową;

§ 3.

Administrator Danych Osobowych Cuiavia Okręgowa Spółdzielnia Mleczarska w Inowrocławiu nie wyznacza Inspektora Danych Osobowych, gdyż zgodnie z art. 37 ogólnego rozporządzenia o ochronie danych nie spełnia przesłanek wynikających z tego przepisu powodujących konieczność jego powołania.

§ 4.

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe określa **załącznik do „Polityki Bezpieczeństwa" nr 1.**

§ 5.

Administrator Danych Osobowych Cuiavia Okręgowa Spółdzielnia Mleczarska w Inowrocławiu prowadzi rejestr czynności przetwarzania danych osobowych, za które odpowiada. W rejestrze tym zamieszczone są informacje wynikające z art. 30 ust. 1 rozporządzenia RODO, a w szczególności:

a) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, jeśli występują,
b) nazwa czynności przetwarzania
c) cele przetwarzania danych osobowych,
d) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych,
e) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych, jeśli występują,
f) planowane terminy usunięcia poszczególnych kategorii danych; jeżeli jest to możliwe do ustalenia,
g) w miarę możliwości, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 rozporządzenia RODO.

Wzór rejestru czynności przetwarzania danych osobowych **(RCPD)** stanowi **załącznik nr 2 do „Polityki Bezpieczeństwa".**

§ 6.

1. **Osoby upoważnione do przetwarzania danych w Cuiavii Okręgowej Spółdzielni Mleczarskiej w Inowrocławiu** dbają o to, aby dane osobowe w formie papierowej i elektronicznej były niedostępne dla osób nieuprawnionych.
2. **Osoby upoważnione do przetwarzania danych w Cuiavii Okręgowej Spółdzielni Mleczarskiej w Inowrocławiu**, do których obowiązków należy pozyskiwanie danych osobowych osób, których dane dotyczą, wypełniają wobec nich obowiązek informacyjny wynikający z art. 13 ogólnego rozporządzenia o ochronie danych.

3. Obowiązek informacyjny wynikający z art. 13 ogólnego rozporządzenia o ochronie danych, Administrator Danych Osobowych wypełnia również poprzez zamieszczenie stosownej informacji dla poszczególnych grup osób, których dane zostały pozyskane, na swojej stronie internetowej: **www.osmcuiavia.pl**.

4. Dokumenty znajdują się w pomieszczeniach oraz szafach i biurkach zamykanych na klucz, do których dostęp mają tylko osoby posiadające aktualne upoważnienie do przetwarzania danych osobowych.

§ 7.

1. Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez **Administratora Danych Osobowych,** które zostały przeszkolone i poinformowane o obowiązkach wynikających z przepisów ogólnego rozporządzenia o ochronie danych i przepisów prawa polskiego oraz pouczone o konsekwencjach wynikających z naruszenia przepisów prawa i wewnętrznych przepisów obowiązujących u **Administratora Danych.** Upoważnienia nadane pracownikom Administratora przechowuje się w ich aktach osobowych.

2. **Administrator Danych stosuje** środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

3. **Administrator Danych** nadaje uprawnienia pracownikom którzy przetwarzają dane poprzez podpisanie upoważnienia, którego wzór stanowi **załącznik nr 3 do „Polityki Bezpieczeństwa"**.

4. Poza RCPD prowadzona jest także dokumentacja opisująca sposób przetwarzania danych w podmiocie, w postaci:

   a) Ewidencja osób przetwarzających dane w podmiocie, posiadających upoważnienie. Wzór ewidencji osób przetwarzających dane osobowe stanowi **załącznik nr 4 do „Polityki Bezpieczeństwa".**

   b) Określenie środków technicznych i organizacyjnych, niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych **- załącznik nr 5 do „Polityki Bezpieczeństwa".**

§ 8.

Na wniosek osoby, której dane dotyczą, Administrator Danych jest obowiązany niezwłocznie nie później jednak niż w terminie 1 miesiąca od dnia otrzymania żądania, udzielić odpowiedzi na to żądanie. Żądanie to, osoba, której dane dotyczą, może skierować przy pomocy formularzy znajdujących się w siedzibie Administratora Danych Osobowych.

§ 9.

Administrator Danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych osobowych w tym podmiocie. Podmiot ten, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie. Administrator prowadzi rejestr podmiotów przetwarzających, którego wzór stanowi **Załącznik nr 6 do „Polityki Bezpieczeństwa"**.

§ 10.

Sposób zabezpieczenia oraz przetwarzania danych w systemie informatycznym reguluje **Instrukcja Zarządzania Systemem Informatycznym, która stanowi załącznik nr 7 do „Polityki Bezpieczeństwa"**

§ 11.

W przypadku naruszenia bezpieczeństwa ochrony danych osobowych Administrator Danych podejmuje wszelkie czynności zgodne z treścią art. 33 i 34 ogólnego rozporządzenia o ochronie danych. Procedura

zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu oraz zawiadamiania osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, zawarta jest w odrębnym dokumencie - **Regulaminie zgłoszenia naruszenia bezpieczeństwa danych osobowych.**

§ 12.

W sprawach nieuregulowanych w niniejszej „Polityce Bezpieczeństwa" mają zastosowanie odpowiednie przepisy **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 orz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)** oraz ustawy o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz.U. nr 1000).

§ 13.

Deklaracja intencji, cele i zakres polityki bezpieczeństwa

1. Administrator Danych wyraża pełne zaangażowanie dla zapewnienia bezpieczeństwa przetwarzanych danych osobowych oraz wsparcie dla przedsięwzięć technicznych i organizacyjnych związanych z ochroną danych osobowych.

2. Polityka określa podstawowe zasady bezpieczeństwa i zarządzania bezpieczeństwem systemów, w których dochodzi do przetwarzania danych osobowych.

3. Polityka dotyczy wszystkich danych osobowych przetwarzanych w podmiocie, niezależnie od formy ich przetwarzania (zbiory ewidencyjne, systemy informatyczne) oraz od tego czy dane są lub mogą być przetwarzane w zbiorach danych.

4. Polityka ma zastosowanie wobec wszystkich komórek organizacyjnych w tym oddziałów, samodzielnych stanowisk pracy i wszystkich procesów przebiegających w ramach przetwarzania danych osobowych.

5. Celem Polityki jest przetwarzanie zgodnie z przepisami danych osobowych przetwarzanych w podmiocie oraz ich ochrona przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy przetwarzaniu danych osobowych oraz przed uszkodzeniem, zniszczeniem lub nieupoważnioną zmianą.

6. Ze względu na nieustannie zmieniające się zagrożenia przetwarzania danych osobowych i zmiany prawa niniejsza polityka może być dokumentem dynamicznie zmieniającym się w czasie. Uaktualnienia procedur ochrony, oprogramowania i innych parametrów stosowanych przy przetwarzaniu danych osobowych znajdują na bieżąco odzwierciedlenie funkcjonalne w niniejszej Polityce.

7. Cele Polityki realizowane są poprzez zapewnienie danym osobowym następujących cech:
   a) poufności - właściwości zapewniającej, że dane nie są udostępniane nieupoważnionym podmiotom;
   b) integralności - właściwości zapewniającej, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   c) rozliczalności - właściwości zapewniającej, że działania podmiotu operującego na danych osobowych mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
   d) ciągłości - zdolności do niezakłóconego ich przetwarzania, bez przerw uniemożliwiających ich udostępnianie osobom upoważnionym
   e) zgodności z prawem, rzetelności i przejrzystości- przetwarzanie zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
   f) prawidłowości – prawidłowe przetwarzanie i w razie potrzeby uaktualnianie danych, poprzez przyjmowanie wszelkich rozsądnych działań aby dane osobowe, które są nieprawidłowe w

świetle celów przetwarzania zostały niezwłocznie usunięte lub sprostowane;
g) minimalizacji - poprzez adekwatne, stosowne oraz ograniczone do tego co niezbędne do celów przetwarzanie

8. Dla skutecznej realizacji Polityki Administrator Danych zapewnia:
   a) odpowiednie do zagrożeń i kategorii danych objętych ochroną, środki techniczne i rozwiązania organizacyjne;
   b) szkolenia w zakresie przetwarzania danych osobowych i sposobów ich ochrony;
   c) kontrolę i nadzór nad przetwarzaniem danych osobowych;
   d) monitorowanie zastosowanych środków ochrony;
   e) ciągłe śledzenie zmieniających się zagrożeń wewnętrznych i zewnętrznych, także uwzględnianie zmieniającego się prawa;
   f) kontrolę i nadzór nad przetwarzaniem danych osobowych przez podmioty trzecie, którym dane zostały udostępnione lub powierzone.

9. Monitorowanie przez Administratora Danych zastosowanych środków ochrony obejmuje m.in. działania użytkowników, naruszanie zasad dostępu do danych, zapewnienie integralności plików oraz ochronę przed atakami zewnętrznymi oraz wewnętrznymi.

10. Administrator Danych lub osoba przez niego upoważniona wdraża wszystkie dokumenty składające się na Politykę Bezpieczeństwa i zapewnia zgodność niniejszej Polityki z przepisami określającymi zasady przetwarzania danych osobowych:
    a) Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w Rozporządzeniem 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)
    b) Ustawy o ochronie danych osobowych z dnia 10 maja 2018 r.
    c) Innymi przepisami mającymi zastosowania przy przetwarzaniu danych osobowych.

Administrator Danych Osobowych

Inowrocław, dnia 15.05.2018 r.