Załącznik nr 1
do zarządzenia nr 65 z dnia 09 września 2024 r
Dyrektora Miejskiego Ośrodka Pomocy Rodzinie w Słupsku

Polityka Ochrony Danych Osobowych

w
Miejskim Ośrodku Pomocy Rodzinie w Słupsku

Wersja 1		**Pieczęć firmowa:**	
Opracował:	**Data:**	**Zatwierdził:**	**Data:**
Piotr Szumko	06.09.2024 r.	DYREKTOR Miejskiego Ośrodka Pomocy Rodzinie w Słupsku Marcin Treder	09.09.2024 r.

SPIS TREŚCI

1. Wstęp ... 3
2. Definicje ... 5
3. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe ... 6
4. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych ... 6
5. Wyznaczenie i zadania IOD, ASI ... 6
6. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych ... 6
7. Procedura reagowania na zagrożenia i incydenty ... 7
8. Procedura udostępnienia danych osobowych ... 7
9. Procedura dostępu podmiotów zewnętrznych ... 7
10. Procedura działań korygujących, informacyjnych i zapobiegawczych ... 7
11. Procedura kontroli systemu ochrony danych osobowych ... 7
12. Procedura tworzenia i prowadzenia rejestru czynności przetwarzania ... 7
13. Sprawozdanie roczne stanu systemu ochrony danych osobowych ... 7
14. Szkolenia użytkowników ... 8
15. Postanowienia końcowe ... 8

1. Wstęp

Celem Polityka Ochrony Danych Osobowych jest zapewnienie ochrony danych osobowych przetwarzanych przez Miejski Ośrodek Pomocy Rodzinie w Słupsku przed wszelakiego rodzaju zagrożeniami, tak wewnętrznymi jak i zewnętrznymi, świadomymi lub nieświadomymi.

Polityka została opracowana zgodnie z wymogami określonymi w :

1. 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. Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych,
3. Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne,
4. aktów wykonawczych wydanych na podstawie w/w ustaw.

Sposoby i zasady zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem zapewnienia ich bezpieczeństwa. określa „Polityka Zarządzania Systemem Informatycznym w Miejskim Ośrodku Pomocy Rodzinie w Słupsku", Dokument ten jest integralną częścią Polityka Ochrony Danych Osobowych w Miejskim Ośrodku Pomocy Rodzinie w Słupsku.

Ochrona danych osobowych jest realizowana poprzez:

1. Zabezpieczenia fizyczne,
2. Procedury organizacyjne,
3. Oprogramowanie systemowe,
4. Aplikacje
5. Użytkowników.

Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:

1. Poufność danych - rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom,
2. Integralność danych - rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
3. Rozliczalność danych - rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,
4. Integralność systemu rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej.
5. Niezaprzeczalność – brak możliwości zanegowania swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie.

Niniejszy dokument jest zgodny z następującymi aktami prawnymi:

1. 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. Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz.1000),
3. Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.

2. Definicje

Przez użyte w Polityce określenia należy rozumieć:

1. **MOPR-** rozumie się przez to Miejski Ośrodek Pomocy Rodzinie w Słupsku
2. **Polityka** – rozumie się przez to Politykę Bezpieczeństwa Ochrony Danych Osobowych w Miejskim Ośrodku Pomocy Rodzinie w Słupsku,
3. **Administrator Danych Osobowych (ADO)** –Miejski Ośrodek Pomocy Rodzinie w Słupsku reprezentowany przez Dyrektora MOPR, decydującego o celach i środkach przetwarzania danych osobowych,
4. **Inspektor Ochrony Danych (IOD)** – osoba odpowiedzialna za organizację ochrony danych osobowych,
5. **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),
6. **Ustawa** – rozumie się przez to ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz.1000),
7. **KRI** - rozumie się przez to ustawę z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne,
8. **Dane osobowe (dane)** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
9. **Zbiór danych** – zestaw danych osobowych posiadający określoną strukturę, prowadzony w/g określonych kryteriów oraz celów,
10. **Usuwanie danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację , która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
11. **Zgoda osoby, której dane dotyczą** – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.
12. **Baza danych osobowych** - zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych np. w pamięci zewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze - rekordów lub obiektów, w których są zapisane dane osobowe,
13. **Przetwarzanie danych** - wykonywanie jakichkolwiek operacji na danych osobowych, np. Zbieranie, utrwalanie, opracowywanie, udostępnianie, zmienianie, usuwanie,
14. **System informatyczny (SI)** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
15. **Administrator systemu (ASI)** - osoba nadzorująca pracę systemu informatycznego oraz wykonująca w nim czynności wymagające specjalnych uprawnień,
16. **Użytkownik** - pracownik Miejskiego Ośrodka Pomocy Rodzinie w Słupsku posiadający uprawnienia do pracy w systemie informatycznym zgodnie z zakresem obowiązków służbowych,
17. **Zabezpieczenie systemu informatycznego** – należy przez to rozumieć wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą,

18. **Nośnik komputerowy (wymienny)** – nośnik służący do zapisu i przechowywania informacji, np. Taśmy, dyskietki, pendrivy, dyski twarde,
19. **Incydent** - naruszenie bezpieczeństwa informacji ze względu na poufność, dostępność i integralność,
20. **Zagrożenie** – potencjalna możliwość wystąpienia incydentu,
21. **Korekcja** – działanie w celu wyeliminowania skutków incydentu,
22. **Działanie korygujące** – jest to działanie przeprowadzane w celu wyeliminowania przyczyny incydentu lub innej niepożądanej sytuacji,
23. **Działanie zapobiegawcze** – jest to działanie, które należy przedsięwziąć, aby wyeliminować przyczyny zagrożenia lub innej potencjalnej sytuacji niepożądanej,
24. **Kontrola** – systematyczna, niezależna i udokumentowana ocena skuteczności systemu ochrony danych osobowych, na podstawie wymagań ustawowych, polityki i Polityki.

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

Szczegółowe rozmieszczenie zbiorów dokumentacji papierowej i elektronicznej, zawierającej dane osobowe, jest opisane wg wzoru stanowiącego *załącznik 1 „Wykaz rozmieszczenia zbiorów danych osobowych przetwarzanych w MOPR".*

4. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

Wykaz zbiorów danych osobowych w postaci dokumentacji papierowej i elektronicznej wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, prowadzony jest wg wzoru stanowiącego *załącznik 2 „Wykaz zbiorów danych osobowych przetwarzanych w MOPR".*

5. Wyznaczenie i zadania IOD, ASI

ADO wyznacza Inspektora Ochrony Danych (IOD) oraz Administratora Systemów Informatycznych (ASI). Wzory dokumentów oraz zakresy zadań dla :
- Inspektora Ochrony Danych są zawarte w *załączniku nr 3 do Polityka Ochrony Danych Osobowych w Miejskim Ośrodku Pomocy Rodzinie w Słupsku.*
- Administratora Systemów informatycznych są zawarte w *załączniku nr 4 do Polityka Ochrony Danych Osobowych w Miejskim Ośrodku Pomocy Rodzinie w Słupsku.*

6. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych, przedstawiono w *załączniku 5 „Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych w MOPR".*

7. Procedura reagowania na zagrożenia i incydenty

Katalog zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie przedstawiono w *załączniku 6 „Procedura reagowania na zagrożenia i incydenty w MOPR".*

8. Procedura udostępnienia danych osobowych

Procedura określa zasady i sposób udostępnienia danych osobowych - *załącznik 7 „Zasady i sposób udostępnienia danych osobowych w MOPR".*

9. Procedura dostępu podmiotów zewnętrznych

Procedury określa zasady bezpiecznego przetwarzania danych osobowych przez podmioty zewnętrzne, gdy cel i zakres tego przetwarzania określa Dyrektor MOPR - *załącznik 8 „Procedura dostępu podmiotów zewnętrznych w MOPR".*

10. Procedura działań korygujących, informacyjnych i zapobiegawczych

Procedury określa czynności związane z: inicjowaniem oraz realizacją działań korygujących, informacyjnych i zapobiegawczych wynikających z zaistnienia incydentów bezpieczeństwa lub zagrożeń systemu ochrony danych osobowych – *załącznik 9 „Procedura działań korygujących ,informacyjnych i zapobiegawczych".*

11. Procedura kontroli systemu ochrony danych osobowych

Procedury określa czynności związane z kontrolą systemu ochrony danych osobowych - *załącznik 10 „Procedura kontroli systemu ochrony danych osobowych".*

12. Procedura tworzenia i prowadzenia rejestru czynności przetwarzania

1. IOD monitoruje wykonanie obowiązku prowadzenia rejestru czynności przetwarzania (art. 30 RODO),
2. Rejestr czynności przetwarzania jest wypełniany przez pracownika(pracowników wskazanych przez ADO i weryfikowany przez ADO,
3. ADO decyduje o konieczności aktualizacji rejestru czynności przetwarzania,
4. Rejestr prowadzony jest według wzoru stanowiącego *załącznik 11- Rejestr czynności przetwarzania*",
5. Rejestr czynności przetwarzania może być prowadzony w formie elektronicznej.

13. Sprawozdanie roczne stanu systemu ochrony danych osobowych

1. Raz w roku IOD przygotowuje sprawozdanie roczne stanu funkcjonowania systemu ochrony danych osobowych,
2. Raport przygotowany jest według wzoru stanowiącego *załącznik 12 Sprawozdanie ODO.* a następnie przedstawiany jest ADO.

14. Szkolenia użytkowników

1. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poddany przeszkoleniu lub zapoznany z polityką/regulaminem ochrony danych osobowych.
2. Za przeprowadzenie szkolenia lub zapoznania polityką/regulaminem ochrony danych osobowych odpowiada IOD po otrzymaniu pisemnego powiadomienia od ADO.
3. Zakres szkolenia/zaznajomienia powinien obejmować przepisy ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz dokumentacją ochrony danych osobowych, obowiązującą u Administratora Danych, a także zobowiązanie się do ich przestrzegania. Szczegółowy zakres szkolenia wraz z listą obecności znajduje się w *załączniku 13 – Plan szkolenia ODO.*
4. Po szkoleniu lub po zapoznaniu się z polityką/regulaminem ochrony danych osobowych, użytkownik zobowiązany jest do podpisania Oświadczenia użytkownika o poufności wg wzoru stanowiącego *załącznik 14 – Oświadczenie użytkownika*).

15. Postanowienia końcowe

1. Polityka jest dokumentem wewnętrznym i nie może być udostępniania osobom postronnym w żadnej formie.
2. Wszystkie regulacje dotyczące systemów informatycznych, określone w Polityce dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.
3. Załączniki do Polityki są aktualizowane na bieżąco i nie wymagają wprowadzenia zarządzeniem Dyrektora MOPR. Wszelkie inne zmiany w Polityce dokonywane są w formie zarządzenia Dyrektora MOPR.
4. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce.
5. Przypadki, nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych.
6. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.
7. Kara dyscyplinarna orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby, zgodnie z ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
8. W sprawach nieuregulowanych w niniejszej „Polityce bezpieczeństwa" 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) oraz Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych,