



Procedura Ochrony Danych i Bezpieczeństwa Informacji

Ośrodek Mediacji i Pomocy Psychologiczno-Pedagogicznej Izabela Krzyszycha

ul. Leyka 7, 10-690 Olsztyn

NIP: 7391054853 | REGON: 511427800

1. Cel procedury

Celem procedury jest zapewnienie właściwej ochrony danych osobowych oraz bezpieczeństwa informacji przetwarzanych w Ośrodku, zgodnie z RODO, ustawą o ochronie danych osobowych oraz zasadami poufności w pracy mediatora i psychologa.

2. Zakres

Procedura dotyczy wszystkich danych osobowych i informacji przetwarzanych w Ośrodku, w formie papierowej oraz elektronicznej.

3. Definicje

Dane osobowe – informacje pozwalające na identyfikację osoby fizycznej.

Dane szczególnych kategorii – m.in. dane dotyczące zdrowia, sytuacji rodzinnej, edukacyjnej (przetwarzane za zgodą lub z mocy prawa).

Administrator – Ośrodek Mediacji i Pomocy Psychologiczno-Pedagogicznej Izabela Krzyszycha.

4. Zasady przetwarzania danych

Dane są przetwarzane zgodnie z zasadami:

- legalności,
- rzetelności i przejrzystości,
- minimalizacji,
- ograniczenia celu i przechowywania,
- integralności i poufności.

5. Obowiązki osób przetwarzających dane

Każda osoba przetwarzająca dane:

- działa wyłącznie w zakresie nadanych uprawnień,
- zachowuje poufność danych,
- stosuje środki bezpieczeństwa określone w procedurze.

6. Uprawnienia dostępu

Dostęp do danych mają wyłącznie osoby upoważnione przez Administratora.

Upoważnienia są rejestrowane i przechowywane w aktach Administratora.

7. Środki techniczne i organizacyjne

Administrator stosuje szczegółowe środki zapewniające bezpieczeństwo danych, w tym:

7.1. Środki organizacyjne

- nadawanie i ewidencjonowanie uprawnień do przetwarzania danych,
- zobowiązanie pracowników i współpracowników do zachowania poufności,
- prowadzenie rejestru osób upoważnionych do przetwarzania danych,
- stosowanie zasady minimalizacji danych (przetwarzane tylko dane niezbędne),
- stosowanie kontroli dostępu fizycznego do pomieszczeń,
- regularne instruktaże i szkolenia wewnętrzne z zakresu RODO.

7.2. Środki techniczne

- hasła o odpowiednim stopniu skomplikowania,
- regularna zmiana haseł,

- blokada komputerów po czasie bezczynności,
- stosowanie oprogramowania antywirusowego i zapór sieciowych,
- szyfrowanie nośników danych, jeśli są używane do transportu informacji,
- wykonywanie kopii zapasowych danych i ich zabezpieczenie.

7.3. Przechowywanie dokumentów

- dokumentacja papierowa przechowywana w zamykanych szafach,
- ograniczony dostęp do pomieszczeń, w których przetwarzane są dane,
- niszczenie dokumentów poprzez niszczarkę o poziomie bezpieczeństwa minimum P-4.

7.4. Komunikacja i transmisja danych

- stosowanie szyfrowanych kanałów komunikacji,
- zakaz przesyłania danych osobowych w niezaszyfrowanych plikach,
- używanie służbowych kont e-mail do celów zawodowych.

7A. Zasady czystego biurka i czystego ekranu

- dokumenty pozostawiane na biurku wyłącznie w trakcie pracy,
- obowiązek zamykania dokumentacji po zakończeniu pracy,
- zakaz pozostawiania danych widocznych na ekranie bez nadzoru.

7B. Nośniki danych i urządzenia mobilne

- zakaz wykorzystywania prywatnych nośników danych bez zgody Administratora,
- obowiązek szyfrowania nośników danych,
- używanie tylko urządzeń zabezpieczonych hasłem lub PIN.
- zabezpieczone hasłem urządzenia elektroniczne,
- regularne aktualizacje oprogramowania,
- przechowywanie dokumentów papierowych w zamkniętych szafach,
- niszczenie dokumentów w niszczarce,
- kopie zapasowe danych przechowywane w sposób bezpieczny.

8. Procedura naruszenia bezpieczeństwa danych

W przypadku naruszenia bezpieczeństwa danych:

1. Zgłoszenie naruszenia do Administratora.
2. Analiza zdarzenia i podjęcie działań naprawczych.
3. W razie konieczności – zgłoszenie naruszenia do PUODO w terminie 72 godzin.
4. Dokumentacja incydentu.

9. Praca zdalna i mobilna

W przypadku pracy poza siedzibą Ośrodka:

- korzystanie z urządzeń zabezpieczonych hasłem,
- zakaz udostępniania urządzeń i dokumentów osobom postronnym,
- używanie bezpiecznych kanałów komunikacji.

10. Archiwizacja i usuwanie danych

- dokumenty są przechowywane zgodnie z polityką retencji,
- dane po okresie przechowywania są niszczone lub anonimizowane.

11. Szkolenia

Osoby przetwarzające dane podlegają szkoleniom z zakresu ochrony danych i bezpieczeństwa informacji.

12. Kontrola i aktualizacja procedury

Administrator dokonuje okresowej kontroli stosowania procedury oraz wprowadza aktualizacje w razie potrzeby.

Data wdrożenia: 30.10.2025

Podpis Administratora: _____