Rydułtowy, dnia 23 lipca 2025 r.

DO.142.000006.2025
DO.ZD.000088.2025

Protokół z wykonania audytu zgodności z przepisami o ochronie danych osobowych i bezpieczeństwa informacji

I Dane podstawowe dotyczące audytu:

1. Audyt przeprowadzono dnia 24 czerwca 2025 r. w Miejskim Ośrodku Pomocy Społecznej przy ulicy Raciborskiej 369 w Rydułtowach (44-280 Rydułtowy) zwanego dalej „MOPS".
2. Administratorem danych osobowych jest MOPS reprezentowany przez dyrektora Sylwię Noworytę (Sylwia Noworyta).
3. Audyt przeprowadzono na podstawie przedstawionych dokumentów, oględzin oraz oświadczenia dyrektora MOPS.
4. Audyt przeprowadził wyznaczony w MOPS Inspektor Ochrony Danych Michał Sobik zwany dalej „IOD".
5. Audyt przeprowadzono w obecności dyrektora MOPS i pracownika MOPS Klaudii Wojtali (Klaudia Wojtala).

II Przedmiot audytu:

Przedmiotem audytu było zbadanie zgodności przetwarzania danych osobowych i bezpieczeństwa informacji z obowiązującymi przepisami prawa na dzień przeprowadzania audytu:

1) 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) zwanego dalej RODO,
2) ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych,
3) elementami rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie *Krajowych Ram Interoperacyjności*, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

III Sposób prowadzenia audytu:

Przeprowadzenie audytu polegało na zastosowaniu listy kontrolnej w MOPS (dokument dołączony do niniejszego protokołu), która zawierała 25 pytania dotyczące przestrzegania ochrony danych osobowych i bezpieczeństwa informacji zgodnie z przepisami obowiązującego prawa. Lista ta dotyczy szeregu zadań z zakresu ochrony danych od sfer zabezpieczeń fizycznych, technicznych, organizacyjnych, wymaganej dokumentacji ochrony danych osobowych, zabezpieczenia systemu informatycznego, zabezpieczeń wewnętrznych danych osobowych.

IV Sprawdzenie objęło zakresem:

1. **Zabezpieczenie budynku i pomieszczeń, w których dochodzi do przetwarzania danych osobowych**: system alarmowy, ochronę fizyczną budynku w tym serwerowni, pomieszczeń biur i referatów - biurek oraz szaf w tym tzw. Politykę czystego biurka i czystego ekranu.
2. **Wymaganą dokumentację ochrony danych osobowych taką jak**: upoważnienia pracowników do przetwarzania danych osobowych, listę obecności dotyczącą szkolenia pracowników z zakresu ochrony danych osobowych i bezpieczeństwa informacji, wzory klauzul informacyjnych dot. art.

13 i 14 RODO oraz ich stosowanie, rejestr incydentów i procedurę ich zgłaszania, Biuletyn Informacji Publicznej, rejestr umów powierzenia przetwarzania danych osobowych.

3. **Zabezpieczenia systemu informatycznego w zakresie takim jak**: zabezpieczenie systemów operacyjnych hasłami i kwestia ich zmian, zapory sieciowe, oprogramowanie antywirusowe, szyfrowanie wysyłanych plików zawierających dane osobowe za pośrednictwem poczty elektronicznej, zabezpieczenie gniazd USB jednostek systemowych.
4. Instalacja monitoringu wizyjnego w placówce, procedury wynoszenia sprzętu komputerowego w tym szyfrowanie dysków.

V Wyniki przeprowadzonego audytu:

1. **W toku przeprowadzonego audytu stwierdzono, że:**
   1) budynek MOPS zabezpieczony poprzez żaluzje antywłamaniowe i alarm antywłamaniowy,
   2) pomieszczenia, w których przetwarzane są dane osobowe zabezpieczono poprzez zamek w drzwiach. Biurka oraz szafy, w których przetrzymywane są dokumenty zawierające dane osobowe zabezpieczone są zamkami na klucz. W wyniku przeprowadzonych czynności przez Inspektora ochrony danych stwierdza się, że wszystkie zamki są sprawne,
   3) tzw. polityka czystego biurka i czystego ekranu jest realizowana w sposób prawidłowy i nie budzi zastrzeżeń na wszystkich stanowiskach pracy,
   4) do przetwarzania danych osobowych dopuszczeni zostali tylko pracownicy upoważnieni przez dyrektora MOPS. Wszystkie upoważnienia do przetwarzania danych osobowych są aktualne na dzień przeprowadzenia audytu,
   5) pracownicy MOPS biorący udział w przetwarzaniu danych osobowych zostali przeszkoleni w zakresie ochrony danych osobowych i bezpieczeństwa informacji w okresie od 23 czerwca do 7 lipca 2025 r. (materiały do zapoznania się wraz z imienną listą potwierdzającą udział w szkoleniu). Szkolenie przygotował wyznaczony w MOPS Inspektor Ochrony Danych Michał Sobik.
   6) wzory stosowanych w MOPS klauzul informacyjnych nie budzą zastrzeżeń. Klauzule informacyjne są stosowane w formie papierowej do wniosków z pomocy społecznej i działu świadczeń rodzinnych i dodatków mieszkaniowych, oświadczeń z pomocy społecznej , wniosków o zasiłek rodzinny, świadczeń rodzinnych, funduszy alimentacyjnych, świadczeń pielęgnacyjnych i rodzinnych oraz na stronie internetowej MOPS i Biuletynie Informacji Publicznej.
2. W MOPS nie funkcjonuje monitoring wizyjny.
3. W MOPS obowiązuje dokument określający zasady postępowania dot. incydentów i naruszeń. Stanowi go Rozdział II § 41 i 42 zarządzenia 29/21 z dnia 5 lipca 2021 ws. Polityki bezpieczeństwa danych osobowych w MOPS. Wykazano, że od czasu przeprowadzenia ostatniego audytu, we wrześniu 2024 r. miało miejsce jedno naruszenie ochrony danych osobowych o niskim ryzyku naruszenia praw i wolności osób fizycznych polegające na utracie w systemie elektronicznym danych 30 osób.
4. Biuletyn Informacji Publicznej MOPS w zakresie ochrony danych osobowych i bezpieczeństwa informacji w tym zamieszczanych dokumentów oraz stosowania anonimizacji i pseudonimizacji nie budzi zastrzeżeń.
5. MOPS prowadzi rejestr umów powierzenia przetwarzania danych osobowych.
6. Zabezpieczenia systemu informatycznego:
   1) logowanie do systemu komputerowego jest zabezpieczone hasłem. System wymusza zmianę haseł co 30 dni.
   2) w systemach używane są zapory sieciowe typu UTM WatchGuard, które posiadają Firewall zabezpieczający dostęp do sieci i systemów,
   3) wszystkie jednostki systemowe (komputery) używane w MOPS mają zainstalowane programy antywirusowe Bitdefender. Licencja obowiązuje do 7 kwietnia 2028 roku,
   4) gniazda USB komputerów w MOPS nie są zablokowane. Pracownicy mają zakaz podłączania dysków zewnętrznych,
   5) kopie zapasowe z serwerów są wykonywane codziennie.
   Serwerownia znajduje się w pomieszczeniu nr 9, które jest zamykane na klucz. Serwerownia jest wspólna z Miejskim Zespołem Obsługi Placówek Oświatowych i Urzędem Stanu Cywilnego.

Dostęp do serwerowni jest możliwy od strony MOPS. Przed serwerownią znajduje się lista wejść do pomieszczenia z podaniem godziny wejścia i wyjścia. W serwerowni znajduje się klimatyzator (sprawny) oraz czujnik dymu.

7. Na podstawie oświadczenia dyrektora MOPS stwierdza się, że pliki zawierające dane osobowe przed wysłaniem drogą poczty elektronicznej są uprzednio szyfrowane za pomocą systemowej funkcji 7-Zip.
8. MOPS jest w posiadaniu 6 urządzeń do niszczenia dokumentów papierowych. Na podstawie prób przeprowadzonych przez IOD stwierdza się, że wszystkie urządzenia są w pełni sprawne.
9. Urządzenie wielofunkcyjne (drukarka, ksero, skan) znajdujące się na korytarzu posiada zabezpieczenie przed nieuprawnionym dostępem – hasło. Pracownicy są zobowiązani zabierać niezwłocznie wydrukowane dokumenty zaraz po przeprowadzonej operacji.
10. Komputery typu laptop nie są wynoszone poza teren MOPS.

VI Opinia Inspektora Ochrony Danych:

Poziom ochrony danych osobowych i bezpieczeństwo informacji w MOPS jest obecnie na dobrym poziomie. Podstawowe dokumenty wymagane przepisami ochrony danych osobowych prowadzone są poprawne. System zabezpieczeń fizycznych oraz systemów komputerowych posiada wystarczające zabezpieczenia.

VII Zalecenia:

Brak.

DYREKTOR
Miejskiego Ośrodka Pomocy Społecznej
w Rydułtowach
mgr Sylwia Nowotyta
podpis dyrektora

Inspektor Ochrony Danych
mgr Michał Sobik
podpis audytora