# Jesteś w organizacji pozarządowej? Zapisz się na szkolenie dla osób z organizacji działających we Wrocławiu lub na rzecz miasta.

## Jak się zapisać?

Rezerwacji miejsca na szkolenie dokonasz poprzez:

* przesłanie ankiety na adres: **karolina.ciechanowicz@um.wroc.pl;**
* jej dostarczenie na adres: **Wydział Partycypacji Społecznej, Wrocław, ulica Gabrieli Zapolskiej 4, pokój 120.**

Kontakt pod numerem telefonu: **71 777 7607**.

## Co jest ważne?

Uwaga! **Ankieta szkoleniowa i informacja o przetwarzaniu danych osobowych RODO powinny być podpisane**. Dodatkowo prosimy o wpisanie daty na obu dokumentach.

**Ze względu na sytuację epidemiologiczną, szkolenia będą się odbywać w trybie online.**

## Harmonogram szkoleń

**2. Jak zabezpieczyć dane osobowe w praktyce? (co robić, czego nie robić)**

Szkolenie online. Link i instrukcje do szkolenia otrzymają Państwo po przesłaniu zgłoszenia z adresem mail na 2 dni przed rozpoczęciem szkolenia. Do obsługi potrzebny jest tylko komputer z dostępem do internetu lub opcjonalnie telefon.

Czas trwania szkolenia: 2 dni – łącznie 10 godzin lekcyjnych

Liczba osób w jednej grupie: do 30 osób

Liczba szkoleń: 1

Terminy szkolenia: 11 i 12 kwietnia 2023 roku w godzinach od 16.45 do 20.30

Ostateczny termin zgłoszeń: 7 kwietnia 2023 roku

KOSZT: BEZPŁATNE

O zakwalifikowaniu na szkolenie zainteresowani zostaną powiadomieni indywidualnie telefonicznie lub na podany adres e-mail.

**PROGRAM**

1. Zabezpieczenie urządzenia elektronicznego (komputer, tablet, telefon):
* zaszyfrowanie pamięci urządzenia,
* zabezpieczanie dostępu do urządzenia,
* tworzenie osobnych kont na urządzeniu,
* konfigurowanie ustawień bezpieczeństwa,
* monitorowanie lokalizacji urządzenia,
* zdalne usuwanie danych z urządzenia.
1. Ochrona danych przechowywanych w plikach różnych formatów:
* ograniczanie dostępu do pliku,
* ograniczanie uprawnień do pliku,
* zaszyfrowanie pliku,
* usuwanie metadanych pliku,
* trwałe usuwanie plików.
1. Ochrona danych podczas korzystania z wirtualnych dysków:
* wybór dostawcy wirtualnego dysku,
* konfiguracja ustawień bezpieczeństwa,
* ograniczanie dostępu do plików,
* ograniczanie uprawnień do plików,
* automatyczne usuwanie plików,
* monitorowanie aktywności użytkowników.
1. Ochrona danych podczas korzystania z poczty elektronicznej:
* wybór dostawcy poczty elektronicznej,
* konfiguracja ustawień bezpieczeństwa,
* konfiguracja szyfrowania wiadomości,
* zasady bezpieczeństwa podczas korespondencji.
1. Ochrona danych przetwarzanych w serwisach serwisów internetowych:
* decyzja o korzystaniu z serwisu internetowego,
* wymagania przepisów prawa,
* warunki licencyjne narzędzia,
* konfiguracja ustawień bezpieczeństwa,
* zasady tworzenia hasła,
* wieloskładnikowe uwierzytelnianie,
* Monitorowanie aktywności.

**Ukończenie szkolenia pozwala na zdobycie zaświadczenia o uczestnictwie w szkoleniu.**