Ochrona danych osobowych

Warszawa, 16.05.2025 r.

Pomoc Techniczna dla Funduszy Europejskich
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
Centrum Koordynacji Projektów Środowiskowych

Podstawy prawne

- 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) – tzw. RODO;
- Ustawa o ochronie danych osobowych
- Norma ISO 27001

W jakim przypadku stosujemy RODO?

RODO nie znajduje zastosowania, gdy:

- dane dotyczą osób prawnych, a nie osób fizycznych (np. nazwa firmy, NIP spółki – o ile nie zawiera danych osoby fizycznej),
- przetwarzanie danych odbywa się w ramach czynności o czysto osobistym lub domowym charakterze (np. lista gości na prywatnej uroczystości),
- przetwarzanie danych jest wykonywane przez organy ścigania lub sądy w ramach działań objętych specjalnymi przepisami (np. postępowanie karne),

Najważniejsze definicje

DANE OSOBOWE - oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

Najważniejsze definicje

PRZETWARZANIE - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką 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;

Najważniejsze definicje

ADMINISTRATOR - to osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który **samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych**.

Przykład:

Organizacja realizująca projekt współfinansowany ze środków UE (np. fundusz EFS, FEnIKS, Erasmus+) jest **administratorem danych uczestników projektu**, ponieważ:

- sam decyduje, **jakie dane** musi zebrać (np. imię, nazwisko, PESEL, wykształcenie, sytuacja zawodowa),

Najważniejsze definicje

PODMIOT PRZETWARZAJĄCY - To jednostka, firma lub organizacja, która **przetwarza dane osobowe w imieniu administratora danych**.

Podmiot przetwarzający **nie decyduje o celach ani sposobach przetwarzania danych** – działa wyłącznie na podstawie instrukcji

Najważniejsze definicje

Przykłady Podmiotów Przetwarzających w projektach unijnych:

- **Dostawcy systemów rekrutacyjnych** i formularzy online (np. platformy rejestracyjne uczestników projektów),
- **Firmy szkoleniowe** prowadzące zajęcia dla uczestników na zlecenie beneficjenta projektu,
- **Zewnętrzne biura rachunkowe** obsługujące projekt pod względem księgowym,
- **Firmy IT** zapewniające infrastrukturę serwerową lub oprogramowanie do obsługi dokumentacji projektowej,

Podstawowe zasady przetwarzania danych osobowych.

- **ZASADA LEGALNOŚCI** – przetwarzanie może być tylko dokonywane na podstawie obowiązujących przepisów, rzetelnie i w sposób przejrzysty dla osoby, której dotyczą;
- **ZASADA CELOWOŚCI** – przetwarzamy dane, gdy tylko ma to swój cel – np. dane kontrahentów, aby wydać im towar, dane pracowników, aby realizować postanowienia umowy o pracę; dodatkowo pobierany dane nam niezbędne – np. nie będzie nam potrzebne nazwisko panieńskie matki kontrahenta albo zestaw przebytych chorób pracownika biurowego,
- **ZASADA ADEKWATNOŚCI** – zbieramy tylko takie dane, które są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane,

Podstawowe zasady przetwarzania danych osobowych.

- **ZASADA OGRANICZONEGO CZASU** – dane osobowe przetwarzamy tylko przez ten czas na jaki są nam potrzebne lub na taki okres jak wynika to z przepisów prawa
- **ZASADA INTEGRALNOŚCI I POUFNOŚCI** – do danych mają dostęp tylko upoważnieni pracownicy i upoważnione osoby z zewnątrz, nikt kto nie jest upoważniony nie ma prawa dostępu do danych, które gromadzi pracodawca, robimy wszystko, aby danych nie utracić, czy bezpodstawnie nie modyfikować;
- **ZASADA POPRAWNOŚCI MERYTORYCZNEJ** – zawsze staramy się mieć aktualne dane osobowe i cały czas monitorujemy ich aktualność;

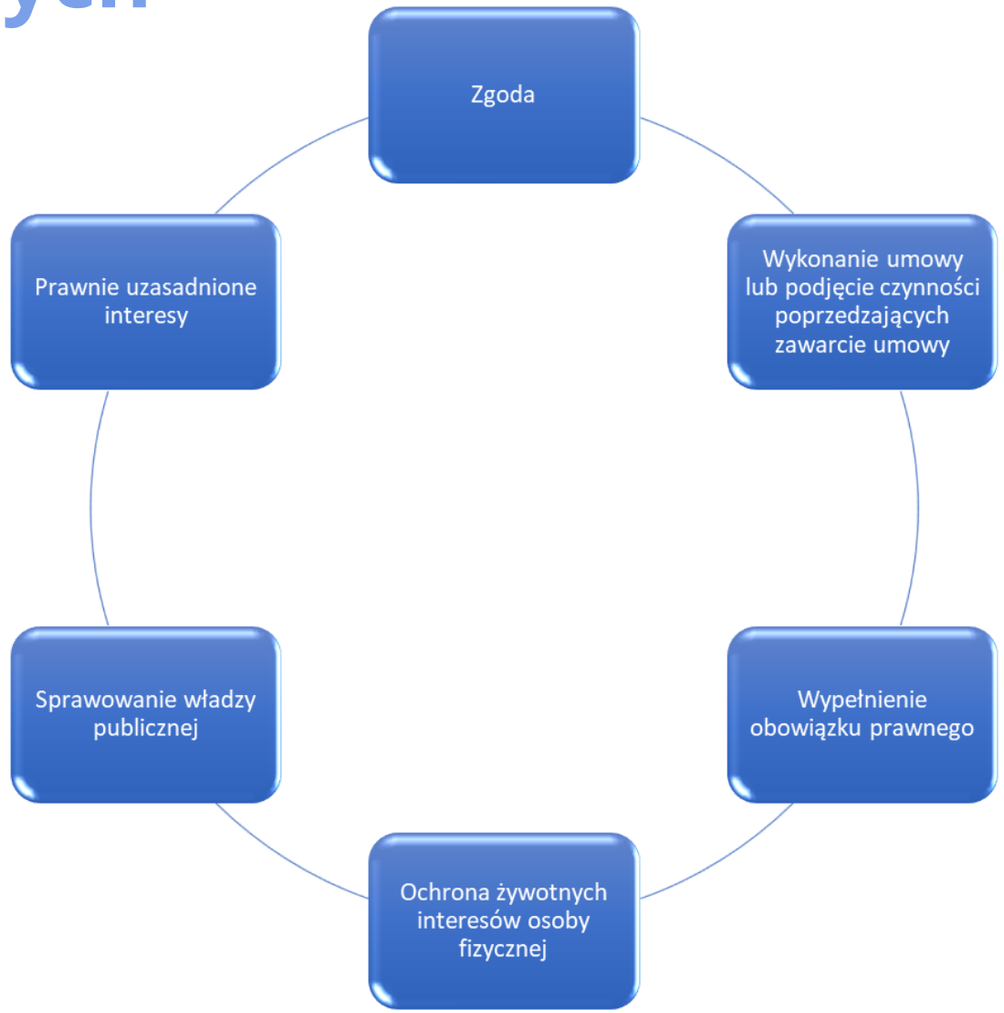
Podstawowe zasady przetwarzania danych osobowych.

- **ZASADA ROZLICZALNOŚCI** – trzeba tak pracować, aby było wiadomo kto dokonał jakich czynności w systemach – każdy korzysta tylko ze swojego stanowiska, wskazanego komputera, swojego loginu, hasła, komputera, telefonu służbowego, aby można było zidentyfikować kto dopuścił się naruszenia i dlaczego oraz musimy umieć wykazać, że przestrzegamy wszystkich zasad.

Rodzaje przetwarzanych danych osobowych

- **Dane osobowe szczególnej kategorii** (wcześniej nazywane danymi wrażliwymi) te dane należy szczególnie chronić: dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.
- **Dane osobowe zwykłe**
  - imię, nazwisko, adres zamieszkania, numer PESEL, numer IP

Podstawy przetwarzania danych osobowych



Kary nałożone przez Prezesa Urzędu Ochrony Danych Osobowych

Z najnowszych danych Urzędu Ochrony Danych Osobowych, wynika, że w 2024 r. zgłoszono

14 722

naruszeń ochrony danych osobowych.

Kary nałożone przez Prezesa Urzędu Ochrony Danych Osobowych

- **Morele.net – 2,8 mln zł**
  Wyrok z 2019 r. – kara za niedostateczne zabezpieczenie danych osobowych klientów (w wyniku ataku hakerskiego wyciekły dane ok. 2,2 mln osób, w tym hasła, adresy i numery telefonów).
- **Towarzystwo Ubezpieczeń Warta S.A. – 85 tys. zł**
  Kara z 2021 r. – za brak zgłoszenia naruszenia ochrony danych oraz niedopełnienie obowiązku informacyjnego wobec osoby, której dane zostały omyłkowo ujawnione innemu klientowi.

Kary nałożone przez Prezesa Urzędu Ochrony Danych Osobowych

- **ALAB Laboratoria – w toku (2023/2024)**
  W wyniku zmasowanego cyberataku dane ok. 200 tys. pacjentów zostały przejęte. UODO prowadzi postępowanie – przewidywana kara może być rekordowa.
- **ClickQuickNow – 2019 r., 201 tys. zł**
  Kara za nieuprawnione wysyłanie wiadomości marketingowych bez zgody i za brak współpracy z UODO podczas kontroli.
- **Virgin Mobile – 1,9 mln zł (2020 r.)**
  Kara za brak odpowiednich środków technicznych do ochrony danych, co umożliwiło nieautoryzowany dostęp do danych klientów.

Co zrobić aby zminimalizować ryzyko naruszenia ochrony danych osobowych?

- Aby zminimalizować ryzyko naruszenia ochrony danych osobowych zachowaj zasadę czystego biurka – chowaj dokumenty, które zawierają dane osobowe, zamykaj je w szafach po skończonej pracy;
- Blokuj ekran monitora po odejściu od biurka;
- Nie zapisuj danych do logowania na kartce przy komputerze (w ogóle nie zapisuj hasła);
- Nie udostępniaj nikomu swoich danych do logowania
- Nie użyczaj sprzętu służbowego osobom trzecim;
- Nie korzystaj z komputera służbowego do celów prywatnych;

Pomoc Techniczna dla Funduszy Europejskich
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
Centrum Koordynacji Projektów Środowiskowych

Odpowiedzialność za naruszenie ochrony danych osobowych.

W stosunku do osoby, która zaniedbuje obowiązki związane z ochroną danych osobowych mogą zostać wyciągnięte konsekwencje:

Dyscyplinarne - przewidziane Kodeksem Pracy oraz wewnętrznymi regulacjami obowiązującymi w strukturze Administratora Danych Osobowych.

Karne - w przypadku, gdy naruszenie miałoby charakter **umyślnego przestępstwa**, wówczas zastosowanie powinny znaleźć **przepisy karne**, a konkretniej art. 107 o ochronie danych osobowych.

Odszkodowawcze – w sytuacji, w której nieprawidłowe przetwarzanie danych przez pracownika narazi pracodawcę na szkodę – np. Gdy pracodawca będzie zobowiązany do wypłaty odszkodowania na rzecz osoby fizycznej, której prawa i wolności zostały naruszone właśnie wskutek niezgodnego z prawem i procedurami działania pracownika.

Zapamiętaj!

Jako pracownik masz obowiązek postępować zgodnie z obowiązującymi w zakładzie pracy:

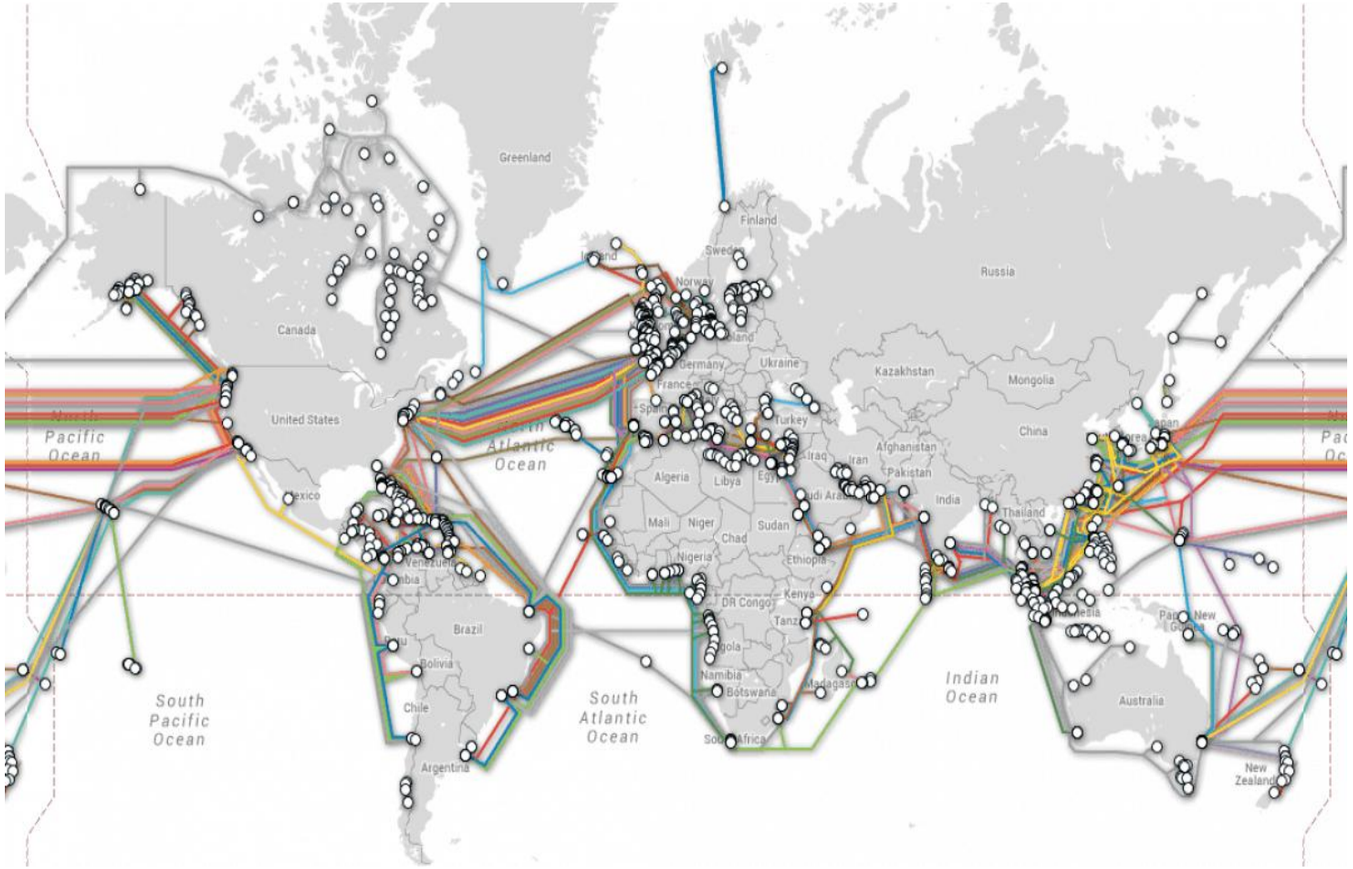
- regulaminami,
- politykami,
- zarządzeniami,

w tym również tymi związanymi z **ochroną danych osobowych i RODO**.

Gdy przetwarzasz dane osobowe w zakresie **przekraczającym** udzielone Ci upoważnienie, przyznane uprawnienia czy w sposób sprzeczny z przyjętymi w organizacji procedurami, wówczas - zgodnie z przepisami kodeksu pracy **- pracodawca ma prawo zastosować** wobec Ciebie karę upomnienia lub nagany. W skrajnych przypadkach niesubordynacja pracownika może zostać uznana za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować nawet **rozwiązaniem umowy w trybie dyscyplinarnym, z winy pracownika.**

Pomoc Techniczna dla Funduszy Europejskich
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
Centrum Koordynacji Projektów Środowiskowych

BEZPIECZEŃSWO INFORMACJI



Pomoc Techniczna dla Funduszy Europejskich
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
Centrum Koordynacji Projektów Środowiskowych

Budowa kabla światłowodowego

Kable światłowodowe mają średnicę około 7 cm, co jest zasługą warstw miedzianych, aluminiowych, olejowych, polietylenowych i stalowych ochronnych.

1 metr waży do około 10 kilogramów.

Pomoc Techniczna dla Funduszy Europejskich
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
Centrum Koordynacji Projektów Środowiskowych

Czym jest bezpieczeństwo informacji?

Bezpieczeństwo informacji to zbiór działań mających na celu **ochronę danych** przed nieautoryzowanym dostępem, ujawnieniem, zmianą, utratą lub zniszczeniem.

Obejmuje trzy kluczowe aspekty:

- **Poufność** – tylko upoważnione osoby mają dostęp do danych,
- **Integralność** – dane są kompletne, dokładne i niezmienione bez upoważnienia,
- **Dostępność** – dane są dostępne wtedy, gdy są potrzebne do działania organizacji.

Jaki są zagrożenia dla bezpieczeństwa informacji?

Bezpieczeństwo informacji może zostać naruszone przez różne czynniki, m.in.:

- **Ataki cybernetyczne**: phishing, ransomware, malware,
- **Błędy ludzkie**: przypadkowe ujawnienie danych, nieprawidłowe adresowanie maili,
- **Zgubienie lub kradzież sprzętu**: np. laptopa lub pendrive'a z danymi,
- **Brak polityk i procedur**: np. nieokreślone zasady dostępu do danych,
- **Awaria techniczna lub katastrofa naturalna**: mogąca prowadzić do utraty danych.

Jak chronić informacje?

- Dobre praktyki w zakresie bezpieczeństwa informacji to:
  - Tworzenie **silnych haseł** i korzystanie z **uwierzytelniania dwuskładnikowego**,
  - **Szyfrowanie danych** na dyskach, w plikach i podczas przesyłania,
  - Regularne wykonywanie **kopii zapasowych** i testowanie ich przywracania,
  - **Szkolenie pracowników** z zakresu RODO i cyberbezpieczeństwa,
  - Ograniczenie dostępu do danych wg zasady **najmniejszych uprawnień (PoLP)**,
  - Stosowanie polityk i procedur bezpieczeństwa oraz **niezwłoczne zgłaszanie incydentów**.

Bezpieczeństwo Informacji

Bezpieczeństwo informacji to odpowiedzialność **każdego pracownika** – niezależnie od stanowiska.

Ochrona danych osobowych i informacji wrażliwych ma kluczowe znaczenie dla funkcjonowania organizacji, jej wiarygodności i zgodności z przepisami prawa (np. RODO).

Pamiętaj:

- Dbaj o **poufność, integralność i dostępność** danych.
- Postępuj zgodnie z **procedurami i politykami bezpieczeństwa**.
- Reaguj szybko i zgłaszaj wszelkie **podejrzenia naruszeń**.
- Regularnie **aktualizuj swoją wiedzę** – cyberzagrożenia stale ewoluują.

Twoja uważność i odpowiedzialność to najlepsza ochrona przed utratą danych.

Pomoc Techniczna dla Funduszy Europejskich
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
Centrum Koordynacji Projektów Środowiskowych

Pytania

Pomoc Techniczna dla Funduszy Europejskich
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
Centrum Koordynacji Projektów Środowiskowych

Pytania

- Czy do rekrutacji uczestników na szkolenia w ramach projektu można (zgodnie z RODO) używać narzędzi takich jak arkusze / ankiety Google? Jeśli tak, pod jakimi warunkami? / jak nie - jakie narzędzia ułatwiające zbieranie danych rekomenduje ekspert (bo potrzebne są nie tylko dane kontaktowe, ale np. czy uczestnik potrzebuje noclegu, kwestie diety / wyżywienia, specjalnych potrzeb)

Pytania

- Kto jest odpowiedzialny za usuwanie danych osobowych (np. uczestników szkół) po upływie okresu trwałości projektu?

Pytania

- „Potrzebuję w łopatologiczny sposób i w telegraficznym skrócie informacji jakie obowiązki dot. RODO obowiązują Beneficjenta, Partnerów i podmioty upoważnione do ponoszenia wydatków podczas realizacji projektu współfinansowanego z FEnIKS. Kto i gdzie jakie dane może przetwarzać i jakie klauzule przy jakich umowach z Wykonawcami powinny być podpisywane.”

Pytania

- W jakich sytuacjach należy zawrzeć umowę powierzenia przetwarzania danych osobowych w projektach unijnych?
- Czy pomiędzy współbeneficjentami należy uregulować zasady przetwarzania danych?

Pytania

- Czy są jakieś odmienne zasady przetwarzania danych osobowych dla projektów w ramach programu LIFE?
- Czy dla pracowników jednostki - osób realizujących zadania w projekcie (w ramach dodatkowych obowiązków) należy wydać odrębne/dodatkowe upoważnienia do przetwarzania danych osobowych dla konkretnego projektu?
- Specjalista ds. zamówień publicznych będzie jednocześnie inspektorem RODO w jednostce, w jaki sposób organizować pracę aby uniknąć konfliktu interesów.

Pytania

- W jaki sposób formułować oświadczenia dotyczące RODO w zapytaniach ofertowych? Jakie informacje powinny się w nich znajdywać?
- Czy lista uczniów zakwalifikowanych do projektu dotyczącego zajęć pozalekcyjnych może zostać udostępniona na stronie internetowej szkoły czy raczej powinny być to numery wniosków?
- Jak zadbać o to, by dane nie trafiły w niepowołane ręce?

Pytania

- Jakie zapisy powinny znaleźć się na umowach personelu zatrudnionego do projektu na umowę o prace lub tez umowę realizacji badań?
- Czym jest rejestr przetwarzania danych, rejestr czynności przetwarzania, rejestr kategorii czynności i karta czynności przetwarzania danych? terminie np. dane uczestników szkoleń.

Pytania

- Jakie zapisy powinniśmy stosować w umowach z Wykonawcami w celu zabezpieczenia interesów osób, których dane są przetwarzana po zakończeniu realizacji umowy, co Wykonawca powinien zrobić ze zgromadzonymi danymi i w jakim terminie np. dane uczestników szkoleń.

Dziękuję za uwagę

Pomoc Techniczna dla Funduszy Europejskich
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
Centrum Koordynacji Projektów Środowiskowych

Autor prezentacji
Magdalena Mistarz

Fundusze Europejskie

Centrum Koordynacji Projektów Środowiskowych
ul. Kolejowa 5/7, 01-217 Warszawa

Pomoc Techniczna dla Funduszy Europejskich

Rzeczpospolita Polska

Dofinansowane przez Unię Europejską

Centrum Koordynacji Projektów Środowiskowych