

RODO



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NCBR
Narodowe Centrum Badań i Rozwoju

POWÓD I CEL POWSTANIA RODO

Przed wprowadzeniem **Rozporządzenia o Ochronie Danych Osobowych (RODO)** w Unii Europejskiej obowiązywały różne przepisy dotyczące ochrony danych osobowych w poszczególnych państwach członkowskich.

RODO powstało jako odpowiedź na rosnące zagrożenia dla prywatności w erze cyfrowej i konieczność ujednolicenia zasad ochrony danych w UE. Dzięki jego wdrożeniu obywatele zyskali większą kontrolę nad swoimi danymi, a organizacje zostały zobowiązane do stosowania bardziej rygorystycznych procedur ochrony informacji. RODO zapewnia **równowagę między prawami jednostek a potrzebami firm i instytucji**, kładąc nacisk na bezpieczeństwo i odpowiedzialność za przetwarzanie danych osobowych.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NCBR
Narodowe Centrum Badań i Rozwoju

AKTY PRAWNE

- Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.
- Ustawa z 10 maja 2018 o ochronie danych osobowych
- Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania RODO
- Ustawa o ochronie danych osobowych przetwarzanych w zw. z zapobieganiem i zwalczaniem przestępczości
- Dyrektywa 2016/680
- 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)

Inne:

- Ustawa o prawach pacjenta i Rzeczniku Praw Pacjenta
- Kodeksy postępowania dla sektora ochrony zdrowia



Fundusze Europejskie
dla Rozwoju Społecznego

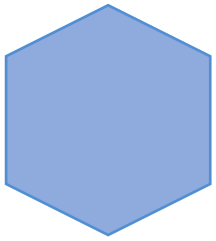


Rzeczpospolita
Polska

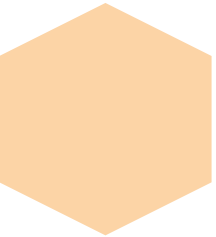
Dofinansowane przez
Unię Europejską



NCBR
Narodowe Centrum Badań i Rozwoju



CO TO SĄ DANE OSOBOWE?



Dane osobowe - oznaczają wszelkie **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. Art. 4 pkt 1 RODO



O danych osobowych mówimy wtedy, gdy informacje umożliwiają identyfikację konkretnej osoby.



Fundusze Europejskie
dla Rozwoju Społecznego

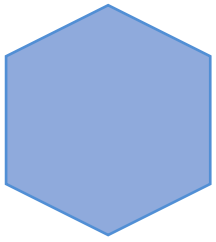


Rzeczpospolita
Polska

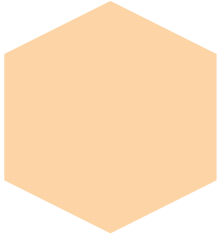
Dofinansowane przez
Unię Europejską



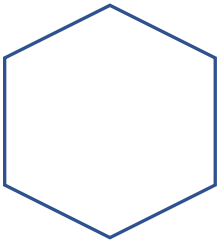
NCBR
Narodowe Centrum Badań i Rozwoju



- Czy coś zostanie uznane za dane osobowe lub nie zależy od **oceny**.
- Identyfikowalność osoby może być względna i uzależniona od tego, kto daną informację przetwarza, w jakim kontekście tego dokonuje oraz jakimi środkami się posługuje.



- Aby stwierdzić, czy dany sposób może być z uzasadnionym prawdopodobieństwem wykorzystany do zidentyfikowania danej osoby, należy wziąć pod uwagę wszelkie obiektywne czynniki, takie jak koszt i czas potrzebne do jej zidentyfikowania, oraz uwzględnić technologię dostępną w momencie przetwarzania danych, jak i postęp technologiczny.



- RODO zawiera zapis, że informacji nie uważa się za **umożliwiającą określenie tożsamości osoby**, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.



Fundusze Europejskie
dla Rozwoju Społecznego

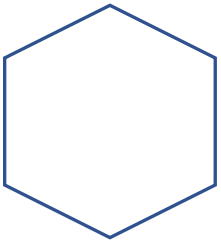
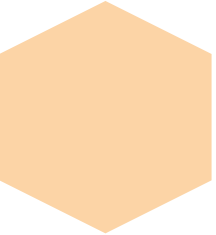
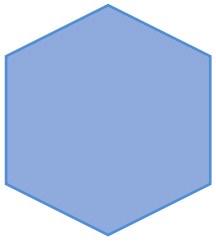


Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NCBR
Narodowe Centrum Badań i Rozwoju



NA CZYM POLEGA PRZETWARZANIE DANYCH OSOBOWYCH?

Przetwarzanie danych osobowych to każda operacja lub zestaw operacji wykonywanych na danych osobowych, niezależnie od tego, czy są one realizowane w sposób zautomatyzowany czy manualny. Obejmuje to m.in.:

- zbieranie,
- utrwalanie,
- organizowanie,
- porządkowanie,
- przechowywanie,
- adaptowanie lub modyfikowanie,
- pobieranie,
- przeglądanie,
- wykorzystywanie,
- ujawnianie poprzez przesłanie, rozpowszechnianie,
- dopasowywanie lub łączenie,
- ograniczanie,
- usuwanie lub niszczenie.



Fundusze Europejskie
dla Rozwoju Społecznego

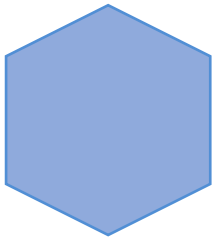


Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



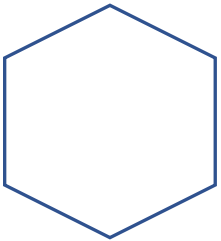
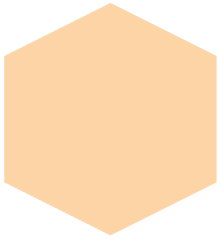
NCBR
Narodowe Centrum Badań i Rozwoju



Rozporządzenie 2016/679 (RODO) – kluczowe regulacje UE w zakresie ochrony danych.

Główne zasady:

- **Zgodność z prawem, rzetelność i przejrzystość** – dane muszą być przetwarzane zgodnie z obowiązującymi przepisami oraz w sposób jasny dla osób, których dotyczą.
- **Ograniczenie celu** – dane mogą być wykorzystywane wyłącznie w określonych celach.
- **Minimalizacja danych** – należy zbierać tylko te informacje, które są rzeczywiście potrzebne.
- **Prawidłowość** – dane muszą być aktualne i poprawne.
- **Ograniczenie przechowywania** – przechowywanie danych powinno trwać tylko przez okres niezbędny do realizacji celu.
- **Integralność i poufność** – należy stosować odpowiednie zabezpieczenia chroniące dane.
- **Rozliczalność** – organizacja musi wykazać, że przestrzega zasad RODO.



Fundusze Europejskie
dla Rozwoju Społecznego

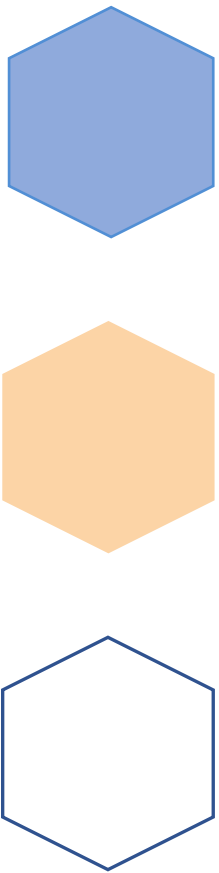


Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NCBR
Narodowe Centrum Badań i Rozwoju



PRZYKŁADY DANYCH OSOBOWYCH

- imię i nazwisko
- adres zamieszkania
- adres e-mail umożliwiający identyfikację jego właściciela (np. zawierający imię i nazwisko+firma)
- numer telefonu komórkowego lub domowego
- PESEL
- dane o lokalizacji (np. ustawienia lokalizacji w telefonie komórkowym)
- adres IP
- dane przechowywane przez szpital lub lekarza, które mogą jednoznacznie wskazywać tożsamość danej osoby

Powyższe informacje mogą wydawać się nieszkodliwe, lecz w rękach nieuprawnionych osób mogą prowadzić do poważnych naruszeń.

Danymi osobowymi nie będą m.in.: numer KRS, firmowy adres e-mail (np. kontakt@firma.pl), anonimowe dane.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NCBR
Narodowe Centrum Badań i Rozwoju

KATEGORIE DANYCH OSOBOWYCH

ZWYKŁE

- PESEL - unikalny dla każdego z nas oraz definicyjnie służy do jednoznacznej identyfikacji osoby fizycznej.
- Adres e-mail – szczególnie jeżeli posiada dane pozwalające zidentyfikować jakąś osobę. Posiadanie adresu email w postaci jan.kowalski@wp.pl nie stanowi danej osobowej, ponieważ niemożliwe jest określenie wyłącznie na jego podstawie tożsamości użytkownika, który się nim posługuje.

Jednak, gdy adres email stworzony został w postaci imie.nazwisko@nazwa_firmy.pl, istnieje duże prawdopodobieństwo jednoznacznego wskazania właściciela i wówczas mówimy, iż adres jest daną osobową.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NCBR
Narodowe Centrum Badań i Rozwoju

KATEGORIE DANYCH OSOBOWYCH

WRAŻLIWE

Dane ujawniające:

- pochodzenie rasowe,
- etniczne,
- poglądy polityczne,
- przekonania religijne,
- światopoglądowe,
- przynależność do związków zawodowych

oraz przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, danych dotyczących seksualności i orientacji seksualnej osoby fizycznej.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NCBR
Narodowe Centrum Badań i Rozwoju

KATEGORIE DANYCH OSOBOWYCH

WRAŻLIWE



Przetwarzanie danych wrażliwych jest niedopuszczalne, chyba że:

- 1) przepisy prawa zezwalają na ich przetwarzanie lub
- 2) jest to niezbędne dla ochrony życia lub zdrowia lub interesów osoby, której dane dotyczą, lub innej osoby, lub
- 3) dane takie zostały upublicznione przez osobę, której dotyczą.

Art. 14 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NCBR
Narodowe Centrum Badań i Rozwoju

KATEGORIE DANYCH OSOBOWYCH

Kiedy można przetwarzać dane wrażliwe?

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679

- a) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu;
- b) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NCBR
Narodowe Centrum Badań i Rozwoju

KATEGORIE DANYCH OSOBOWYCH

Kiedy można przetwarzać dane wrażliwe?

- c) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;
- d) przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NCBR
Narodowe Centrum Badań i Rozwoju

KATEGORIE DANYCH OSOBOWYCH

Kiedy można przetwarzać dane wrażliwe?

- e) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;
- f) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;
- g) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NCBR
Narodowe Centrum Badań i Rozwoju

KATEGORIE DANYCH OSOBOWYCH

Kiedy można przetwarzać dane wrażliwe?

- h) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń, o których mowa w ust. 3;



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NCBR
Narodowe Centrum Badań i Rozwoju

KATEGORIE DANYCH OSOBOWYCH

Kiedy można przetwarzać dane wrażliwe?

3. Dane osobowe, o których mowa w ust. 1, mogą być przetwarzane do celów, o których mowa w ust. 2 lit. h), jeżeli są przetwarzane przez – lub na odpowiedzialność – pracownika podlegającego obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe lub przez inną osobę również podlegającą obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NCBR
Narodowe Centrum Badań i Rozwoju

KATEGORIE DANYCH OSOBOWYCH

Kiedy można przetwarzać dane wrażliwe?

- i) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową;



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NCBR
Narodowe Centrum Badań i Rozwoju

KATEGORIE DANYCH OSOBOWYCH

Kiedy można przetwarzać dane wrażliwe?

- j) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NCBR
Narodowe Centrum Badań i Rozwoju

OBOWIĄZKI WZGLĘDEM DANYCH OSOBOWYCH W ORGANIZACJI

OBOWIĄZKI ADMINISTRATORA DANYCH

- **Zapewnienie zgodności z przepisami RODO** - wdrożenie środków organizacyjnych i technicznych zapewniających zgodność z RODO.
- **Powołanie Inspektora Ochrony Danych (IOD)** - powołanie IOD jest obowiązkowe wtedy, gdy przetwarzanie danych odbywa się na dużą skalę. Inspektor pełni funkcję doradczą i kontrolną, monitorując zgodność z przepisami RODO, prowadząc szkolenia oraz współpracując z Urzędem Ochrony Danych Osobowych (UODO). IOD powinien posiadać odpowiednie kwalifikacje i być niezależny w realizacji swoich zadań.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NCBR
Narodowe Centrum Badań i Rozwoju

OBOWIĄZKI WZGLĘDEM DANYCH OSOBOWYCH W ORGANIZACJI

OBOWIĄZKI ADMINISTRATORA DANYCH

- **Prowadzenie rejestru czynności przetwarzania** – rejestr zawiera informacje o kategoriach danych, celach ich przetwarzania, podstawach prawnych oraz odbiorcach danych. Rejestr pomaga w identyfikacji ryzyk i zapewnieniu zgodności z zasadami RODO, a także może być wymagany podczas kontroli UODO.
- **Realizacja obowiązku informacyjnego** - każdy ma prawo do informacji o tym, kto przetwarza jego dane, w jakim celu, przez jaki czas i na jakiej podstawie prawnej. Administrator musi spełniać ten obowiązek poprzez przekazanie klauzuli informacyjnej (np. w formie papierowej lub elektronicznej). W przypadku zbierania danych nie bezpośrednio od osoby, obowiązek ten musi zostać zrealizowany w rozsądnym terminie, nie później niż w ciągu miesiąca.



OBOWIĄZKI WZGLĘDEM DANYCH OSOBOWYCH W ORGANIZACJI

OBOWIĄZKI ADMINISTRATORA DANYCH

- **Zabezpieczenie danych** - ochrona danych osobowych wymaga zastosowania środków technicznych (np. szyfrowania, kontroli dostępu, pseudonimizacji) oraz organizacyjnych (np. polityk bezpieczeństwa, szkoleń pracowników). Organizacje muszą także wdrożyć procedury reagowania na incydenty związane z naruszeniem danych oraz zgłaszać je do UODO w ciągu 72 godzin od wykrycia.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NCBR
Narodowe Centrum Badań i Rozwoju

OBOWIĄZKI PROCESORA

Podmiot przetwarzający dane osobowe na zlecenie administratora, ma określone obowiązki zgodnie z RODO. Do jego głównych zadań należą:

- **Przetwarzanie danych wyłącznie na polecenie administratora** – procesor nie może wykorzystywać danych do własnych celów.
- **Zapewnienie odpowiednich środków ochrony danych** – procesor musi wdrożyć odpowiednie zabezpieczenia techniczne i organizacyjne.
- **Prowadzenie rejestru czynności przetwarzania** – jeśli jest to wymagane przez RODO.
- **Współpraca z administratorem** – procesor musi umożliwić administratorowi spełnianie obowiązków wynikających z RODO, np. przy realizacji praw osób, których dane dotyczą.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NCBR
Narodowe Centrum Badań i Rozwoju

OBOWIĄZKI PROCESORA

- **Pomoc w zapewnieniu zgodności z przepisami o ochronie danych** – w tym przy ocenach skutków dla ochrony danych (DPIA).
- **Zgłaszanie naruszeń ochrony danych** – procesor powinien niezwłocznie informować administratora o każdym incydencie związanym z bezpieczeństwem danych.
- **Zawarcie umowy powierzenia przetwarzania** – każda współpraca między administratorem a procesorem powinna być uregulowana umową.
- **Nieangażowanie podprocesorów bez zgody administratora** – jeśli procesor chce powierzyć przetwarzanie dalszemu podmiotowi, musi uzyskać zgodę administratora.



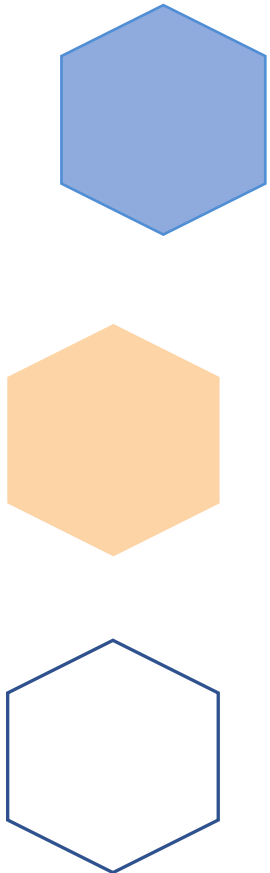
ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH

Zgoda na przetwarzanie danych osobowych to jedna z podstaw prawnych przetwarzania danych zgodnie z RODO. Musi być **dobrowolna, świadoma, konkretna i jednoznaczna**, a osoba, której dane dotyczą, powinna mieć możliwość jej wycofania w dowolnym momencie.

Co powinna zawierać zgoda?

- **Tożsamość administratora danych** – nazwa i dane kontaktowe podmiotu przetwarzającego dane.
- **Cel przetwarzania danych** – jasne określenie, w jakim celu dane będą wykorzystywane.
- **Zakres przetwarzanych danych** – informacje, jakie dane będą gromadzone i przetwarzane.
- **Podstawa prawna przetwarzania** – odniesienie do przepisów RODO.
- **Prawo do wycofania zgody** – informacja, że osoba może w dowolnym momencie odwołać zgodę bez negatywnych konsekwencji.
- **Podpis osoby wyrażającej zgodę** – potwierdzenie świadomego wyrażenia zgody.





ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

- **Zasada legalności, rzetelności i przejrzystości** - przetwarzanie danych musi odbywać się zgodnie z prawem, uczciwie i w sposób zrozumiały dla osoby, której dane dotyczą.
- **Zasada ograniczenia celu** - dane mogą być zbierane i wykorzystywane wyłącznie w określonym, wyraźnym i zgodnym z prawem celu.
- **Zasada minimalizacji danych** - przetwarzane dane powinny być adekwatne, stosowne i ograniczone do niezbędnego minimum.
- **Zasada prawidłowości** - dane muszą być dokładne i aktualne, administrator ma obowiązek ich poprawiania lub usuwania, jeśli są błędne.
- **Zasada ograniczenia przechowywania** - dane powinny być przechowywane jedynie przez okres niezbędny do realizacji celu ich przetwarzania.
- **Zasada integralności i poufności** - dane muszą być zabezpieczone przed nieuprawnionym dostępem, utratą, zniszczeniem lub uszkodzeniem.
- **Zasada rozliczalności** - administrator danych musi być w stanie wykazać zgodność przetwarzania z zasadami RODO oraz spełnianie obowiązków wynikających z przepisów.



Fundusze Europejskie
dla Rozwoju Społecznego

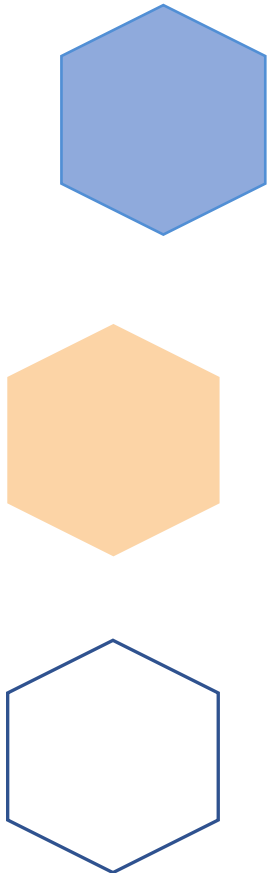


Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NCBR
Narodowe Centrum Badań i Rozwoju



ZABEZPIECZENIA PRZETWARZANIA DANYCH OSOBOWYCH

Środki organizacyjne - procedury i zasady zapewniające zgodność przetwarzania danych z RODO, np. polityki ochrony danych, regulaminy bezpieczeństwa, szkolenia pracowników oraz prowadzenie rejestru czynności przetwarzania. Kluczowe jest także określenie ról i odpowiedzialności, np. powołanie Inspektora Ochrony Danych (IOD).

Środki techniczne – stosowanie technologii ochrony, takie jak szyfrowanie, pseudonimizacja, zabezpieczenia sieciowe (np. zapory ogniowe i systemy wykrywania włamań), a także mechanizmy uwierzytelniania i kontroli dostępu (np. logowanie wieloskładnikowe). Systemy informatyczne muszą być regularnie aktualizowane i testowane pod kątem podatności na ataki, a dane przechowywane w sposób chroniący je przed nieuprawnionym dostępem, modyfikacją lub usunięciem.

Środki nadzorcze - wdrożenie mechanizmów monitorowania zgodności z przepisami, w tym do regularnego przeprowadzania audytów bezpieczeństwa oraz analiz ryzyka. Organy nadzorcze mają prawo do kontroli przestrzegania przepisów oraz nakładania sankcji w przypadku wykrycia naruszeń.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NCBR
Narodowe Centrum Badań i Rozwoju

NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Naruszenie ochrony danych osobowych to incydent prowadzący do nieuprawnionego dostępu, ujawnienia, utraty, zniszczenia lub zmiany danych osobowych. Może to dotyczyć zarówno danych cyfrowych, jak i papierowych.

Przykłady naruszeń:

- Utrata lub kradzież dokumentów zawierających dane osobowe.
- Nieautoryzowany dostęp do systemów informatycznych.
- Wysłanie danych osobowych do niewłaściwego odbiorcy.
- Ataki hakerskie, ransomware, phishing.
- Ujawnienie danych osobom nieupoważnionym.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NCBR
Narodowe Centrum Badań i Rozwoju

NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Obowiązki administratora w przypadku naruszenia

- Zgłoszenie naruszenia do Urzędu Ochrony Danych Osobowych (UODO) w ciągu **72 godzin** od wykrycia incydentu.
- Poinformowanie osób, których dane dotyczą – jeśli naruszenie może skutkować wysokim ryzykiem dla ich praw i wolności.
- Podjęcie działań naprawczych, np. zmiana haseł, wdrożenie dodatkowych zabezpieczeń.
- Dokumentowanie wszystkich naruszeń, nawet jeśli nie wymagają zgłoszenia do UODO.

Konsekwencje naruszeń

- Kary finansowe – UODO może nałożyć kary do 20 milionów euro lub 4% rocznego obrotu firmy.
- Odpowiedzialność prawna – osoby poszkodowane mogą dochodzić odszkodowania.
- Utrata zaufania – szkody wizerunkowe dla organizacji, placówki medycznej lub firmy.



NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Zapobieganie naruszeniom

- Regularne szkolenia personelu.
- Stosowanie silnych haseł i wielopoziomowej autoryzacji.
- Szyfrowanie i anonimizacja danych.
- Opracowanie procedur reagowania na incydenty i testowanie zabezpieczeń.
- Monitorowanie dostępu do danych i systemów informatycznych.

Ocena ryzyka polega na identyfikacji i analizie potencjalnych zagrożeń związanych z przetwarzaniem danych osobowych, w szczególności pod kątem ich poufności, integralności i dostępności. Administratorzy danych są zobowiązani do przeprowadzania analizy ryzyka, aby wdrożyć odpowiednie środki techniczne i organizacyjne minimalizujące prawdopodobieństwo naruszeń ochrony danych. Wysoka ocena ryzyka może skutkować koniecznością przeprowadzenia **Oceny Skutków dla Ochrony Danych (DPIA-Data Protection Impact Assessment)**, zwłaszcza w przypadku przetwarzania danych wrażliwych lub na dużą skalę.



Fundusze Europejskie
dla Rozwoju Społecznego

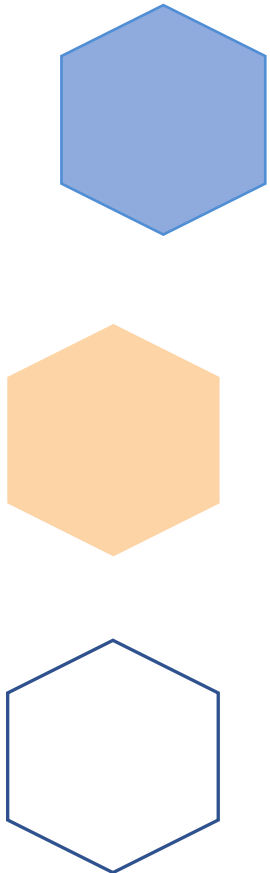


Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



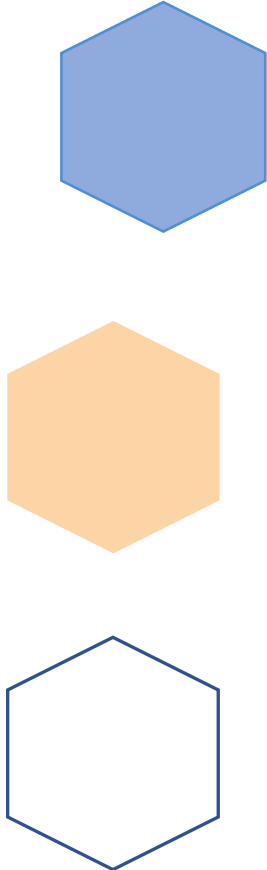
NCBR
Narodowe Centrum Badań i Rozwoju



PRAWA OSÓB, KTÓRYCH DANE OSOBOWE SĄ PRZETWARZANE

- **Prawo do bycia zapomnianym** – umożliwia osobie żądanie usunięcia jej danych osobowych, jeśli nie są już one niezbędne do celów, dla których zostały zebrane, lub gdy wycofała zgodę na ich przetwarzanie. Istnieją jednak wyjątki, np. gdy dane muszą być przechowywane z powodów prawnych.
- **Prawo do przenoszenia danych osobowych** – daje możliwość otrzymania swoich danych w ustrukturyzowanym formacie i ich przekazania innemu administratorowi, jeśli przetwarzanie odbywa się na podstawie zgody lub umowy oraz w sposób zautomatyzowany.
- **Prawo do sprzeciwu** – pozwala osobie sprzeciwić się przetwarzaniu jej danych w określonych sytuacjach, np. gdy są one wykorzystywane do celów marketingowych lub na podstawie uzasadnionego interesu administratora.
- **Postępowanie z żądaniami osób** – administrator danych ma obowiązek odpowiedzieć na żądania osób w określonym terminie (zwykle w ciągu miesiąca) i poinformować je o podjętych działaniach. Jeśli odmówi spełnienia żądania, musi uzasadnić swoją decyzję





DOKUMENTACJA ZWIĄZANA Z PRZETWARZANIEM ORAZ OCHRONĄ DANYCH OSOBOWYCH

Obowiązki dokumentacyjne – obejmują prowadzenie i aktualizowanie dokumentacji związanej z przetwarzaniem danych osobowych.

- **Rejestr Czynności Przetwarzania** – dokument zawierający informacje o celach, podstawach prawnych, kategoriach danych oraz odbiorcach danych osobowych.
- **Rejestr Kategorii Czynności Przetwarzania** – prowadzony przez podmioty przetwarzające dane w imieniu administratora, zawierający informacje o powierzonych mu danych.
- **Polityka Ochrony Danych Osobowych** – dokument określający zasady ochrony danych w organizacji, w tym stosowane środki zabezpieczeń.
- **Instrukcja Zarządzania Systemem Informatycznym** – opisuje zasady przetwarzania danych w systemach IT, w tym procedury dostępu i zabezpieczeń.
- **Analiza Ryzyka i Ocena Skutków dla Ochrony Danych (DPIA)** – dokument oceniający ryzyko związane z przetwarzaniem danych oraz jego wpływ na prywatność osób.



Fundusze Europejskie
dla Rozwoju Społecznego

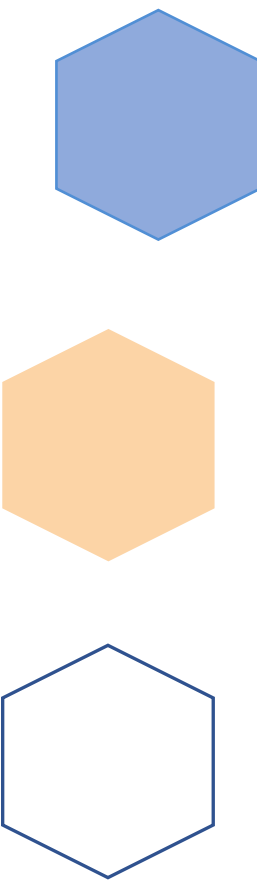


Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NCBR
Narodowe Centrum Badań i Rozwoju



DOKUMENTACJA ZWIĄZANA Z PRZETWARZANIEM ORAZ OCHRONĄ DANYCH OSOBOWYCH

- **Ewidencja Naruszeń Ochrony Danych Osobowych** – dokumentacja incydentów związanych z ochroną danych, w tym podjętych działań zaradczych.
- **Procedura Postępowania w Przypadku Naruszenia Ochrony Danych Osobowych** – instrukcja opisująca sposób reagowania na incydenty związane z ochroną danych.
- **Umowy Powierzenia Przetwarzania Danych** – dokumenty regulujące przekazywanie danych do innych podmiotów przetwarzających (np. firm outsourcingowych).
- **Polityka Retencji Danych** – określająca czas przechowywania danych osobowych w organizacji.
- **Polityka Bezpieczeństwa Informacji** – dokument dotyczący ogólnych zasad ochrony informacji, w tym danych osobowych.



Fundusze Europejskie
dla Rozwoju Społecznego



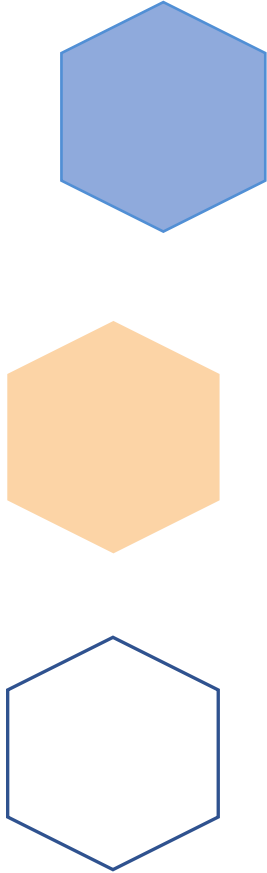
Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NCBR

Narodowe Centrum Badań i Rozwoju



DOKUMENTACJA ZWIĄZANA Z PRZETWARZANIEM ORAZ OCHRONĄ DANYCH OSOBOWYCH

Obowiązki informacyjne – administrator danych osobowych jest zobowiązany do prowadzenia odpowiedniej dokumentacji i udostępniania jej osobom, których dane są przetwarzane. Do kluczowych dokumentów należą:

- **Klauzule Informacyjne RODO** – zawierają informacje wymagane przez art. 13 i 14 RODO, takie jak cel i podstawa prawna przetwarzania danych, okres przechowywania, prawa osób oraz dane kontaktowe administratora i inspektora ochrony danych (jeśli został powołany). Mogą występować w różnych wersjach, np.: klauzula informacyjna dla pracowników, dla klientów, czy dotycząca monitoringu wizyjnego.
- **Polityka Prywatności** – dokument dostępny np. na stronie internetowej administratora, informujący użytkowników o sposobach przetwarzania ich danych, zakresie zbieranych informacji i przysługujących im prawach.
- **Rejestr Realizacji Obowiązku Informacyjnego** – dokument, w którym administrator rejestruje przypadki spełnienia obowiązku informacyjnego wobec różnych grup osób, np. pracowników, klientów czy użytkowników strony internetowej.



Fundusze Europejskie
dla Rozwoju Społecznego

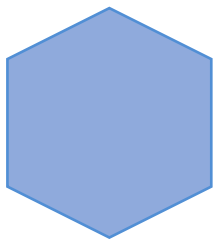


Rzeczpospolita
Polska

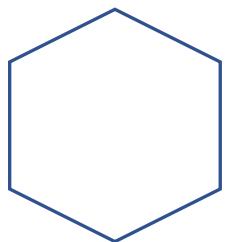
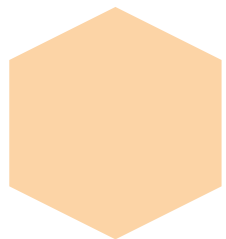
Dofinansowane przez
Unię Europejską



NCBR
Narodowe Centrum Badań i Rozwoju



DOKUMENTACJA ZWIĄZANA Z PRZETWARZANIEM ORAZ OCHRONĄ DANYCH OSOBOWYCH



- **Formularze Zgód na Przetwarzanie Danych Osobowych** – zawierające wyraźne zgody na przetwarzanie danych w określonych celach, np. w celach marketingowych czy rekrutacyjnych. Powinny być zgodne z zasadą dobrowolności i jednoznaczności zgody.
- **Rejestr Wycofanych Zgód** – dokument, w którym administrator odnotowuje przypadki wycofania zgody przez osoby, których dane są przetwarzane.
- **Informacje o Przetwarzaniu Danych w Umowach** – klauzule informujące o przetwarzaniu danych osobowych zawarte w umowach z kontrahentami, pracownikami i innymi podmiotami.
- **Procedura Realizacji Praw Osób, Których Dane Dotyczą** – określająca sposób, w jaki administrator realizuje obowiązek informacyjny oraz odpowiada na wnioski osób dotyczące dostępu, sprostowania, usunięcia czy przeniesienia ich danych.



Fundusze Europejskie
dla Rozwoju Społecznego

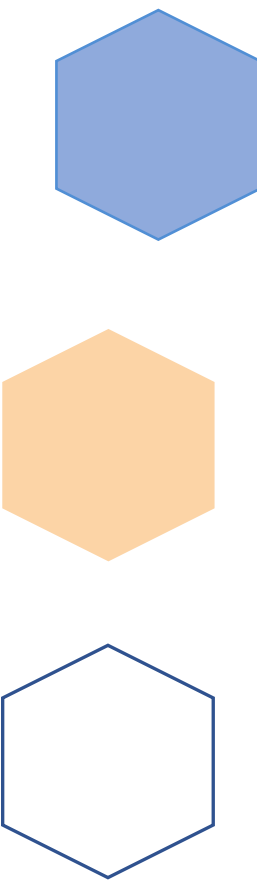


Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NCBR
Narodowe Centrum Badań i Rozwoju



DOKUMENTACJA ZWIĄZANA Z PRZETWARZANIEM ORAZ OCHRONĄ DANYCH OSOBOWYCH

Upoważnienia w zakresie RODO – administrator danych osobowych powinien prowadzić odpowiednią dokumentację, aby zapewnić kontrolę nad dostępem do danych i zgodność z przepisami.

- **Upoważnienia do Przetwarzania Danych Osobowych** – indywidualne dokumenty nadawane pracownikom lub współpracownikom, określające zakres ich dostępu do danych osobowych oraz cel ich przetwarzania.
- **Rejestr Upoważnień do Przetwarzania Danych Osobowych** – dokument zawierający listę osób, które otrzymały upoważnienie, wraz z datami jego nadania i ewentualnego cofnięcia.
- **Procedura Nadawania i Odwoływania Upoważnień** – określa sposób przyznawania oraz cofania upoważnień do przetwarzania danych, a także zakres odpowiedzialności osób upoważnionych.



Fundusze Europejskie
dla Rozwoju Społecznego

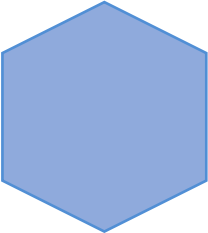


Rzeczpospolita
Polska

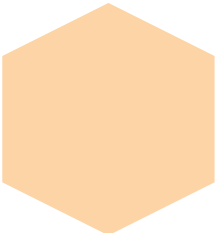
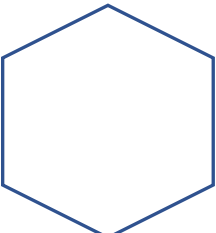
Dofinansowane przez
Unię Europejską



NCBR
Narodowe Centrum Badań i Rozwoju



DOKUMENTACJA ZWIĄZANA Z PRZETWARZANIEM ORAZ OCHRONĄ DANYCH OSOBOWYCH

- 
- **Lista Osób Upoważnionych do Przetwarzania Danych w Systemach Informatycznych** – zestawienie pracowników i innych osób, które mają dostęp do danych w systemach IT, wraz z zakresem ich uprawnień.
 - **Rejestr Cofniętych Upoważnień** – dokumentacja dotycząca wycofanych upoważnień, zawierająca daty oraz przyczyny cofnięcia dostępu do danych osobowych.
 - **Procedura Nadawania i Odwoływania Upoważnień** – określa sposób przyznawania oraz cofania upoważnień do przetwarzania danych, a także zakres odpowiedzialności osób upoważnionych.
 - **Oświadczenie o Zachowaniu Poufności** – podpisywane przez osoby upoważnione do przetwarzania danych osobowych, zobowiązujące je do przestrzegania zasad ochrony danych i poufności.
- 



Fundusze Europejskie
dla Rozwoju Społecznego

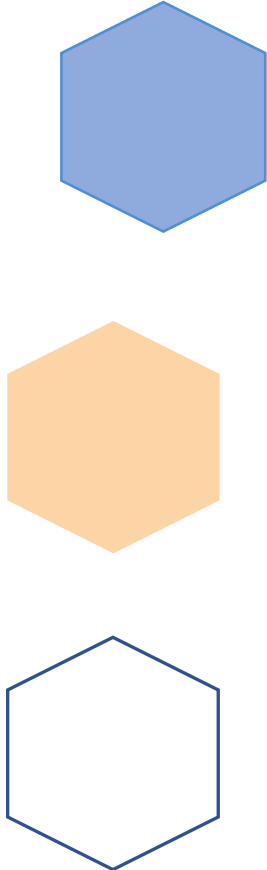


Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NCBR
Narodowe Centrum Badań i Rozwoju



OPERACJE PRZETWARZANIA DANYCH OSOBOWYCH

Rodzaje czynności przetwarzania danych osobowych można podzielić na kilka podstawowych kategorii w zależności od ich celu i sposobu wykonywania. Każda z nich obejmuje konkretne działania, jakie administrator lub podmiot przetwarzający wykonuje na danych osobowych.

1. **Zbieranie danych.** To pierwszy etap przetwarzania – gromadzenie informacji od osób fizycznych. Może odbywać się np. poprzez: wypełnianie formularzy (np. rejestracja w sklepie internetowym, zapis do newslettera), przesyłanie CV w procesie rekrutacji, podawanie danych podczas rozmowy telefonicznej.
2. **Utrwalanie i przechowywanie danych.** Gdy dane zostaną już zebrane, muszą być odpowiednio zapisane i przechowywane, np.: w bazach danych systemów informatycznych, w plikach papierowych (np. umowy w segregatorach), na serwerach chmurowych lub lokalnych, w archiwach i rejestrach firmowych.
3. **Organizowanie i porządkowanie danych.** Przetwarzanie często wymaga uporządkowania danych, np.: kategoryzowanie danych według określonych kryteriów (np. klientów według lokalizacji), grupowanie danych w bazach klientów lub pracowników, nadawanie etykiet czy identyfikatorów do łatwiejszej obsługi.



Fundusze Europejskie
dla Rozwoju Społecznego

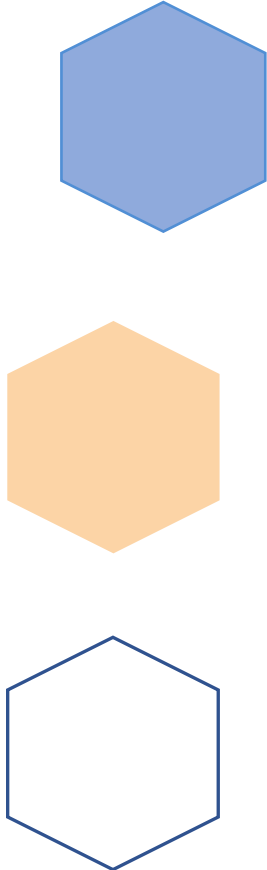


Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NCBR
Narodowe Centrum Badań i Rozwoju



OPERACJE PRZETWARZANIA DANYCH OSOBOWYCH

4. **Modyfikacja i aktualizacja danych.** Administrator lub użytkownik może edytować dane, np.: poprawiać błędy literowe w nazwiskach, zmieniać adres zamieszkania lub numer telefonu, dodawać nowe informacje, np. o statusie zamówienia, łączyć dane z różnych źródeł w celu ich uaktualnienia.
5. **Wykorzystywanie danych.** Przetwarzanie danych może służyć do ich aktywnego użycia, np.: wykorzystywanie danych klientów do personalizowania ofert, analizowanie historii zakupów w celu lepszego dopasowania reklam, profilowanie użytkowników na podstawie ich zachowań, analizowanie wyników badań i raportów w firmach.
6. **Udostępnianie i przekazywanie danych.** Czasem dane są przekazywane innym podmiotom lub osobom trzecim, np.: wysyłanie danych klientów do firm kurierskich w celu dostarczenia przesyłki, przekazywanie danych do biura rachunkowego, które obsługuje płace pracowników, udostępnianie informacji instytucjom publicznym (np. urzędowi, policji), jeśli jest to wymagane przez prawo.



Fundusze Europejskie
dla Rozwoju Społecznego

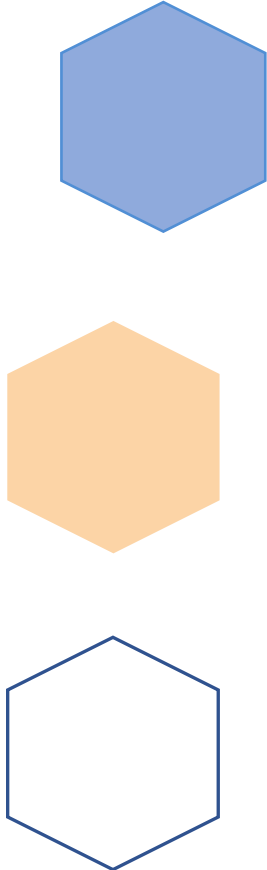


Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NCBR
Narodowe Centrum Badań i Rozwoju



OPERACJE PRZETWARZANIA DANYCH OSOBOWYCH

7. **Ograniczanie przetwarzania danych.** W niektórych przypadkach dane nie są usuwane, ale ich przetwarzanie zostaje czasowo ograniczone, np.: blokowanie danych w bazie na czas rozpatrywania reklamacji, wstrzymywanie przetwarzania danych na wniosek osoby, której dane dotyczą, gdy sprawdzana jest ich poprawność.
8. **Usuwanie i niszczenie danych.** Dane mogą być usuwane, gdy nie są już potrzebne, np.: usunięcie konta użytkownika z serwisu internetowego, likwidacja dokumentacji papierowej poprzez jej zniszczenie, trwałe usunięcie plików z serwerów i baz danych, anonimizacja danych, co oznacza ich trwałe przekształcenie tak, aby nie można było ich przypisać do konkretnej osoby.

Techniki ochrony prywatności:

Anonimizacja – całkowite usunięcie danych osobowych lub ich tak silna zmiana, że nie można ich przypisać do konkretnej osoby (np. zamiana nazwisk na losowe identyfikatory).

Pseudonimizacja – częściowe ukrycie danych, np. zamiana nazwisk na unikalne kody, ale z możliwością ich późniejszego przywrócenia, jeśli jest to konieczne.



Fundusze Europejskie
dla Rozwoju Społecznego

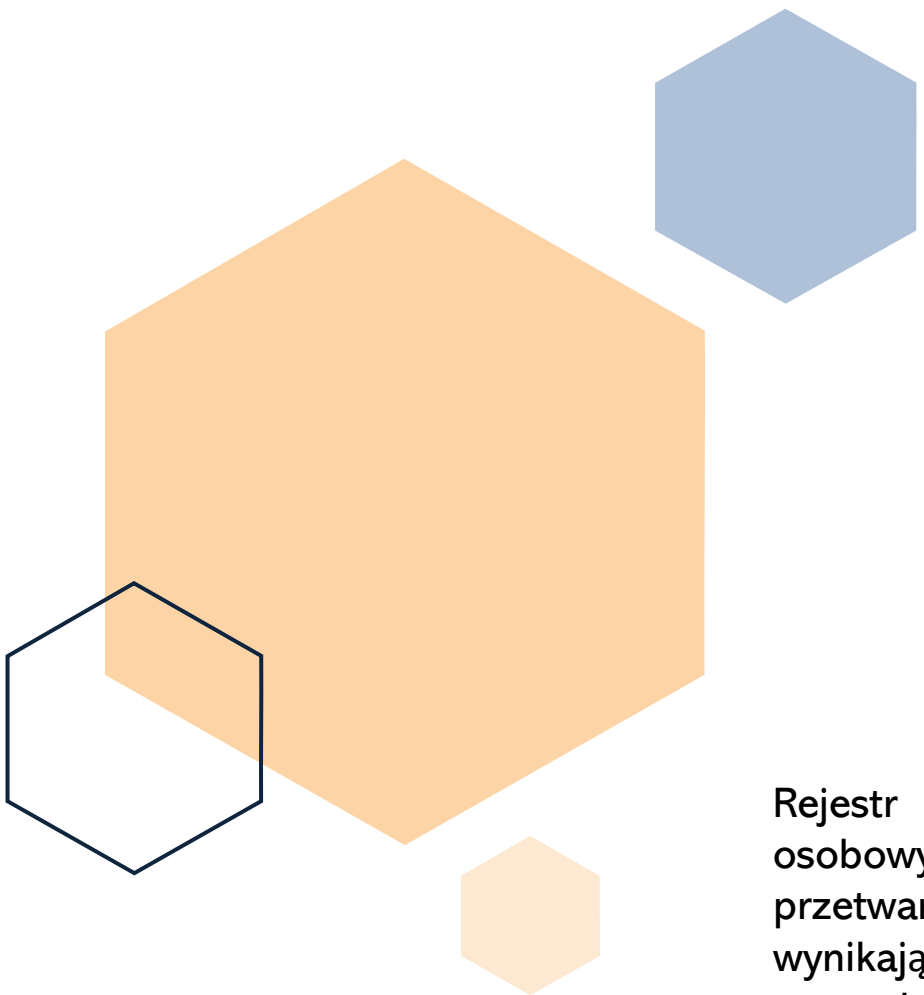


Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NCBR
Narodowe Centrum Badań i Rozwoju



REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

Obowiązek prowadzenia tzw. Rejestru czynności przetwarzania danych osobowych spoczywa na ściśle określonych w RODO podmiotach, m.in. **zatrudniających ponad 250 pracowników**, ale także takich, które **przetwarzają dane osobowe szczególnej kategorii**, a takimi są przetwarzane w placówkach medycznych **dane osobowe (wrażliwe) dotyczące stanu zdrowia pacjentów**.

Rejestr służy do udowodnienia zachowania zgodności przetwarzania danych osobowych z wytycznymi RODO. Umożliwia również inwentaryzację zasobów przetwarzanych danych, a także ułatwia weryfikację realizacji obowiązków wynikających z przepisów o ochronie danych osobowych. Rejestr może być prowadzony w formie pisemnej lub elektronicznej, np. arkusza programu Excel.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NCBR
Narodowe Centrum Badań i Rozwoju

REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

W rejestrze muszą się znaleźć:

- 1) informacje pozwalające na identyfikację i nawiązanie kontaktu: imię i nazwisko/ nazwa oraz dane kontaktowe, a także wszelkich współadministratorów, a także, gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych;
- 2) cele przetwarzania;
- 3) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
- 4) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NCBR
Narodowe Centrum Badań i Rozwoju

REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

- 5) gdy ma to zastosowanie, informacje dotyczące przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazania, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń;
- 6) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
- 7) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (m.in. dotyczących pseudonimizacji i szyfrowania danych, zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania danych).



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NCBR
Narodowe Centrum Badań i Rozwoju



NADZÓR, KONTROLA I DORADZTWO W ZAKRESIE OCHRONY DANYCH OSOBOWYCH

Ochrona danych osobowych w organizacjach podlega nadzorowi zarówno ze strony organów państwowych, jak i wewnętrznych specjalistów ds. ochrony danych. Kluczowe role w tym zakresie pełnią **Urząd Ochrony Danych Osobowych (UODO)** oraz **Inspektor Ochrony Danych (IOD)**.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NCBR
Narodowe Centrum Badań i Rozwoju

Urząd Ochrony Danych Osobowych (UODO)

UODO to organ państwowy odpowiedzialny za kontrolę przestrzegania przepisów RODO w Polsce. Do jego głównych zadań należą:

- monitorowanie i egzekwowanie przepisów o ochronie danych osobowych,
- przeprowadzanie kontroli w organizacjach przetwarzających dane,
- rozpatrywanie skarg osób, których dane są przetwarzane,
- nakładanie kar administracyjnych za naruszenia RODO,
- prowadzenie działań edukacyjnych i wydawanie wytycznych dotyczących ochrony danych.

W przypadku stwierdzenia naruszeń UODO może nakazać zmianę sposobu przetwarzania danych, a także nałożyć kary finansowe.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NCBR
Narodowe Centrum Badań i Rozwoju

Inspektor Ochrony Danych (IOD)

IOD to osoba wyznaczona w organizacji do nadzorowania przestrzegania przepisów o ochronie danych. Nie każda firma musi powołać IOD – obowiązek ten dotyczy m.in. podmiotów publicznych oraz firm przetwarzających dane na dużą skalę (np. szpitale, banki). Do jego zadań należy:

- doradztwo w zakresie ochrony danych osobowych,
- monitorowanie przestrzegania przepisów RODO w organizacji,
- przeprowadzanie szkoleń dla pracowników,
- współpraca z UODO w razie kontroli,
- udzielanie odpowiedzi na pytania osób, których dane są przetwarzane.

IOD działa niezależnie i nie może być karany za wykonywanie swoich obowiązków. Jest kluczowym punktem kontaktowym między organizacją a UODO oraz osobami, których dane są przetwarzane.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NCBR
Narodowe Centrum Badań i Rozwoju

ODPOWIEDZIALNOŚĆ W KONTEKŚCIE RODO

RODO nakłada obowiązki na wszystkie podmioty przetwarzające dane osobowe, a ich niewłaściwe przetwarzanie może prowadzić do poważnych konsekwencji prawnych i finansowych.

Odpowiedzialność za zgodność z przepisami ponoszą **administratorzy danych**, **podmioty przetwarzające** oraz, w określonych przypadkach, **pracownicy mający dostęp do danych**.

Za naruszenia RODO grożą **kary finansowe**, które mogą sięgać nawet **20 mln euro** lub **4% rocznego obrotu firmy**. Poza sankcjami administracyjnymi, osoby poszkodowane mogą dochodzić **odszkodowania**, a w skrajnych przypadkach przewidziana jest również odpowiedzialność karna (np. za bezprawne udostępnianie danych).

Właściwa ochrona danych i przestrzeganie RODO jest więc nie tylko obowiązkiem prawnym, ale także kluczowym elementem budowania zaufania klientów i partnerów biznesowych.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NCBR
Narodowe Centrum Badań i Rozwoju

PODSUMOWANIE

- W jaki sposób RODO chroni nas jako osoby, których dane osobowe są przetwarzane?
- Czy Reforma RODO wpłynęła korzystnie na proces ochrony danych osobowych?
- Z jakiego powodu RODO w instytucji jest koniecznym do wykorzystania aktem prawnym?



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NCBR
Narodowe Centrum Badań i Rozwoju

Dziękuję

