# Analiza zgodności z RODO

RODO jest skrótem od Rozporządzenia o Ochronie Danych Osobowych (ang*. General Data Protection Regulation* - GDPR). Jest to 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). Weszło ono w życie 25 maja 2018 r.

## Definicje wykorzystywanych pojęć

Podczas analizy zgodności systemu z RODO konieczna jest znajomość wykorzystywanych w ustawie pojęć. Jest ona niezbędna do poprawnego zrozumienia wymagań stawianych systemowi wynikających z tego rozporządzenia. W tym celu

***„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

„***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

**„ograniczenie przetwarzania”** oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania

**„profilowanie”** oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

**„pseudonimizacja”** oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej

**„zgoda**” osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych

**„naruszenie ochrony danych osobowych”** oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych

## Prezentacja wymagań i rozwiązań

W tej części zawarto kolejny wymagania stawiane przed systemem, które wynikają z obowiązywania RODO oraz przyjęte rozwiązania odnoszące się do tych wymagań.

**Wymaganie 1: Privacy by design**

Zgodnie z Art. 25 ust.1:

*Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą.*

**Wymaganie 2: Privacy by default**

Zgodnie z Art. 25 ust.2:

*Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych*

**Realizacja 1+2:** System nie zbiera na temat użytkowników danych nie mających zastosowania przy jego działaniu. Zminimalizowana jest ilość danych wymaganych przy tworzeniu konta użytkownika w serwisie. Podanie dodatkowe informacje dotyczących użytkownika jest możliwe poprzez edycje profilu użytkownika i jest całkowicie dobrowolne. Dane użytkownika wykorzystywane są przez system rekomendacji, który przedstawia użytkownikowi spersonalizowane propozycje pubów do odpowiedzenia, jeżeli użytkownik wyrazi na to zgodę. 0 W bazie danych zawierającej dane osobowe użytkowników zastosowany jest mechanizm pseudonimizacji.

**Wymaganie 3: Brak możliwości przetwarzania, zbierania i przechowywania danych osobowych bez jednej z podstawy wskazanych w przepisach**

Zgodnie z Art. 6. Podstawy do przetwarzania danych to:

* umowa - przetwarzanie jest niezbędne do wykonania umowy
* zgoda wyrażona przez osobę, której dane dotyczą
* wypełnienie obowiązku prawnego
* realizacja prawnie uzasadnionych interesów administratora danych

**Realizacja 3:** Podstawą przetwarzania danych w systemie jest zgoda użytkownika. System przetwarza dane osobowe użytkownika jedynie w wypadku wyrażenia zgody przez użytkownika. Zgoda ta uzyskana jest w sposób prawidłowy, co opisuje *Wymaganie 4*.

**Wymaganie 4: Pozyskanie zgody od użytkownika w sposób prawidłowy**

Zgodnie z Art.7:

*1. Jeżeli przetwarzanie odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych.*

*2. Jeżeli osoba, której dane dotyczą, wyrażą zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Część takiego oświadczenia osoby, której dane dotyczą, stanowiąca naruszenie niniejszego rozporządzenia nie jest wiążąca.*

*3. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie.*

*4. Oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy między innymi od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy*

Oznacz to, że:

• zgoda pozyskana musi być zawsze przed rozpoczęciem przetwarzania danych

• sposoby wyrażania zgody: pisemna, ustna; klarowne, potwierdzające czynność działanie

• automatyczne zaznaczanie zgody jest zabronione

• zgoda musi dotyczyć przetwarzania konkretnych danych, w konkretnym czasie, w konkretnym celu

• obowiązuje zakaz łączenia zgód na przetwarzanie danych

• zgoda musi być wyrażona bez przymusu

• zgoda musi być poparta rzetelną klauzulą informacyjną

• nie jest wyrażeniem zgody: milczenie, okienka domyślnie zaznaczone, niepodjęcie działania itp.

**Rozwiązanie 4:** Zgoda użytkownika na przetwarzanie jego danych osobowych uzyskiwana jest podczas jego rejestracji w systemie. System wyświetla użytkownikowi zapytanie o zgodę na wykorzystanie jego danych osobowych. Zapytanie to spełnia wymienione powyżej warunki. Rezygnacja ze zgodny przebiega w prosty sposób i jest możliwa poprzez jej odznaczenie w profilu użytkownika po zalogowaniu.

**Wymaganie 5: Prawo użytkownika do przeniesienia danych**

RODO wprowadza prawo osoby, której dane dotyczą do przeniesienia jej danych osobowych do innego administratora. Osoba, której dane są przetwarzane może poprosić o przekazanie danych wskazanemu przez nią podmiotowi. Dane należy przekazać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego (np. XML czy CSV).

**Rozwiązanie 5:** W aplikacji webowej podane są dane kontaktowe do administracji serwisu. Prośbę o przeniesienie danych do innego administratora należy wysłać na adres mailowy wskazany w danych kontaktowych. W treści wiadomości należy umieści token (kod), który uwierzytelni użytkownika. Token ten można wygenerować w profilu użytkownika po zalogowaniu. Mechanizm ten służy zwiększeniu bezpieczeństwa.

**Wymaganie 6: Prawo użytkownika do bycia zapomnianym**

Prawo do bycia zapomnianym to prawo do usunięcia danych. Osoba, której dotyczą dane ma prawo zażądać od administratora danych usunięcia dotyczących jej danych, a żądanie to musi być spełnione jeśli nie występują przesłanki, które to uniemożliwiają.

Bez wątpienia należy usunąć dane m.in. jeśli:

* nie są już one niezbędne do celów, w których zostały zebrane
* zgoda na podstawie, której przetwarzałeś dane została cofnięta
* dane były przetwarzane niezgodnie z prawem
* dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego (np. w ramach portalu społecznościowego)

Są jednak sytuacje, w których możliwa jest odmowa spełnienia żądania usunięcia danych. Ma to miejsce m.in. jeśli przetwarzanie tych danych jest niezbędne:

* do wywiązania się z prawnego obowiązku
* do ustalenia, dochodzenia lub obrony roszczeń
* do korzystania z prawa do wolności wypowiedzi i informacji

**Rozwiązanie 6:** W aplikacji webowej podane są dane kontaktowe do administracji serwisu. Prośbę o usunięcie danych należy wysłać na adres mailowy wskazany w danych kontaktowych. W treści wiadomości należy umieści token (kod), który uwierzytelni użytkownika. Token ten można wygenerować w profilu użytkownika po zalogowaniu. Mechanizm ten służy zwiększeniu bezpieczeństwa.

**Wymaganie 7: Prawo użytkownika do żądania ograniczenia przetwarzania danych**

**Wymaganie 8: Prawo użytkownika do otrzymania kopii danych**

**Wymaganie 9: Prawo użytkownika do sprzeciwu wobec profilowania**

**Wymaganie 10: Przejrzystość języka**

Zabronione jest używanie trudnych, specjalistycznych sformułowań, tak samo jak utrudnianie zapoznania się z ważnymi informacjami, np. stosowania w komunikatach tzw. metody „drobnego druczku”.

**Rozwiązanie 10:** Tekst zgód napisany jest w przystępnej i zrozumiałej formie. Przejrzystość działania serwisu jest częścią jednego z wymagań niefunkcjonalnych serwisu = „zapewnienie możliwie najlepszego User Experience.