

Ośrodek Pomocy Społecznej
21-025 Niemce, ul. Lubelska 119
NIP 7131096205, Regon 004168110
tel. 81 501-52-21, fax 81 756-10-29

Analiza ryzyka dla przetwarzania danych osobowych w Centralnym Rejestrze Umów dla Ośrodka Pomocy Społecznej W Niemcach

Metryka dokumentu - do uzupełnienia przez jednostkę

Nazwa jednostki	Ośrodek Pomocy Społecznej
Administrator danych	Ośrodek Pomocy Społecznej w Niemcach
Komórka odpowiedzialna za CRU	Dział organizacyjny- administracyjny
Właściciel procesu / koordynator CRU	Ośrodek Pomocy Społecznej
Inspektor ochrony danych	Natalia Pietruszka
Osoby / stanowiska upoważnione do pracy w CRU	Starszy inspektor Elżbieta Kroczy; referent Sylwia Gziut
Data sporządzenia / aktualizacji analizy	30.06.2026
Wersja dokumentu	1
Osoba sporządzająca	Natalia Pietruszka
Osoba zatwierdzająca	Kierownik Ośrodka Pomocy Społecznej Barbara Ścisł
Data kolejnego przeglądu	30.06.2027

1. Ustalenie kontekstu przetwarzania danych

Zgodnie z art. 34a ust. 1 Ustawy z 27.08.2009 r. o finansach publicznych (Dz.U. z 2025 r., poz. 1483 ze zm. – dalej: u.f.p.), kierownik jednostki sektora finansów publicznych ma obowiązek udostępniania i aktualizowania w Centralnym Rejestrze Umów Jednostek Sektora Finansów Publicznych (dalej: CRU) informacji o umowach zawartych przez jednostkę sektora finansów publicznych (dalej: j.s.f.p.) lub na jej rzecz. Realizacja tego obowiązku wymaga przetwarzania danych osobowych, dlatego w niniejszym dokumencie przeprowadzona zostanie analiza ryzyka naruszenia praw i wolności osób, których dane dotyczą związanego z przetwarzaniem danych osobowych, zgodnie z art. 24 i art. 32 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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 (Dz. Urz. UE. L. z 2016 r., poz. 119) – dalej: ogólne rozporządzenie o ochronie danych.

Informacje o umowach, w tym dane osobowe, będą wprowadzane do systemu teleinformatycznego CRU przez osoby upoważnione przez kierownika j.s.f.p. Analiza ryzyka dotyczyć będzie przetwarzania danych osobowych w zakresie informacji o umowach zamieszczanych w CRU w imieniu kierownika jednostki. Dane osobowe udostępniane w CRU są gromadzone w Ośrodku Pomocy Społecznej, pochodzą z umów zawieranych przez jednostkę z kontrahentami (wykonawcami umów).

W zakresie zapewnienia funkcjonowania systemu teleinformatycznego, w którym jest prowadzony CRU, administratorem danych użytkowników kont w systemie oraz innych danych w zakresie, w jakim jest to niezbędne do zapewnienia funkcjonowania systemu jest Minister Finansów, który ma obowiązek przeprowadzenia analizy ryzyka i przyjęcia odpowiednich zabezpieczeń, dlatego ten obszar przetwarzania danych nie będzie objęty niniejszą analizą.

2. Opis przetwarzanych danych i ich klasyfikacja

W CRU udostępniane będą dane osobowe osoby, z jaką Ośrodek Pomocy Społecznej w Niemcach zawarła umowę odpłatną zawieraną między zamawiającym a wykonawcą, której przedmiotem jest nabycie przez zamawiającego od wybranego wykonawcy robót budowlanych, dostaw lub usług oraz która została zawarta w formie pisemnej, dokumentowej, elektronicznej albo innej formie szczególnej, bez względu na wartość przedmiotu umowy, z wyjątkami odnoszącymi się do umów określonych w art. 34a ust. 5 u.f.p., w tym m.in. umów z zakresu prawa pracy. W CRU nie udostępnia się informacji o umowie, co do których prawo do informacji publicznej podlega ograniczeniu na podstawie art. 5 ust. 1 i 2-2b ustawy z 6.09. 2001 r. o dostępie do informacji publicznej (Dz.U. z 2022 r. poz. 902, dalej u.d.i.p.). CRU jest jawny, prowadzony w systemie teleinformatycznym i umożliwia wyszukiwanie informacji o umowie udostępnionych w CRU oraz wgląd do tych informacji.

Do danych osobowych, które będą udostępniane w CRU należą informacje o osobach fizycznych z którymi zawarte zostały umowy finansowane ze środków publicznych. (np. dane osoby fizycznej, z którą gmina zawarła umowę zlecenia). Przepis art. 34a ust. 7 u.f.p. wśród informacji podlegających udostępnianiu wskazuje „oznaczenie stron umowy” (pkt 4). Zgodnie z §3 pkt 2 rozporządzenia Ministra Finansów i Gospodarki z 30.03.2026 r. w sprawie Centralnego Rejestru Umów Jednostek Sektora Finansów Publicznych (Dz.U. z 2026 r., poz. 440, dalej: rozporządzenie CRU), oznaczenie stron umowy obejmuje a) nazwę (firmę), numer REGON, numer identyfikacji podatkowej (NIP), jeżeli został zamieszczony w bazie REGON, i adres siedziby albo adres wykonywania działalności gospodarczej - w przypadku gdy stroną umowy jest j.s.f.p. lub przedsiębiorca z siedzibą albo miejscem wykonywania działalności gospodarczej - w przypadku gdy stroną umowy jest osoba fizyczna. W CRU wpisywane będą zarówno informacje identyfikujące przedsiębiorców, w tym osób fizycznych prowadzących działalność gospodarczą, jak też informacje o osobach fizycznych, które działalność gospodarczej nie prowadzą, a z którymi zawarta została umowa. W przypadku przedsiębiorców będących osobami fizycznymi zakres danych osobowych jest szerszy i obejmuje ich firmę oraz adres, natomiast w odniesieniu do osób fizycznych, nieprowadzących działalności gospodarczej, zakres informacji udostępnianych w CRU jest wąski i zawiera jedynie imię i nazwisko, natomiast nie powinno się publikować innych danych (w szczególności numerów PESEL, adresów zamieszkania, czy też innych danych osobowych, które są zawarte w umowach).

Z realizacją obowiązku udostępniania i aktualizacji informacji w CRU wiąże się także przetwarzanie danych osobowych kierownika jednostki oraz osób przez niego upoważnionych. Zakres danych tych osób obejmuje imię i nazwisko oraz stanowisko służbowe. Jednak w zakresie przetwarzania danych tych osób w systemie teleinformatycznym CRU administratorem jest właściwy minister, do którego obowiązków należy przeprowadzenie analizy ryzyka przetwarzania tego rodzaju danych osobowych.

Dane osobowe będą wprowadzane do CRU za pośrednictwem komputerów w jednostce, z wykorzystaniem oprogramowania i kont dostępowych udostępnianych przez administratora systemu teleinformatycznego CRU. Na administratorze systemu ciąży obowiązek odpowiedniego zabezpieczenia systemu i oprogramowania w zakresie ochrony integralności oraz dostępności danych przetwarzanych w systemie. Informacje prawidłowo udostępnione w CRU mają charakter jawny, jednak do czasu ich publikacji, a także w zakresie danych źródłowych, danych nadmiarowych, dokumentów roboczych, upoważnień, danych kont użytkowników oraz danych niepodlegających udostępnieniu, jednostka zapewnia ich poufność, integralność i dostępność zgodnie z art. 32 RODO.

3. Opis stosowanych zabezpieczeń

Z przetwarzaniem danych osobowych w CRU może wiązać się ryzyko wynikające w szczególności z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych. Stosownie do zagrożeń podjęte zostały odpowiednie środki mające na celu ograniczenie ryzyka.

Dane osobowe przetwarzane w związku z realizacją obowiązku udostępniania informacji w CRU są zabezpieczone z wykorzystaniem następujących rodzajów zabezpieczeń:

- zabezpieczenia organizacyjne – przyjęta została Procedura ochrony danych osobowych przy prowadzeniu CRU, upoważnione do pobierania kluczy do pomieszczeń, w których przetwarza się dane są jedynie osoby uprawnione;
- zabezpieczenia osobowe – uprawnienia do pracy w systemie CRU nadawane są wybranym pracownikom, dokonywana jest weryfikacja tych uprawnień, nadawane są upoważnienia do przetwarzania danych osobowych;
- zabezpieczenia techniczne - programowe: dostęp do systemu CRU przyznawany jest jedynie uprawnionym użytkownikom i wymaga uwierzytelnienia; komputery wyposażone są w oprogramowanie typu firewall oraz oprogramowanie antywirusowe, programy są na bieżąco aktualizowane;
- zabezpieczenia techniczne – fizyczne: dostęp do pomieszczeń w których przetwarzane są dane jest ograniczony, pomieszczenia są zamykane, papierowe nośniki, z których dane wprowadzane są do systemu CRU są przechowywane w zamkniętych szafach.

KIEROWNIK
Ośrodka Pomocy Społecznej
w Niemcach
mgr Barbara Ścisiel

4. Określenie kryteriów akceptacji ryzyka

Poziom ryzyka to iloczyn prawdopodobieństwa zdarzenia i jego skutku. W niniejszej analizie ryzyka w zakresie określenia kryteriów akceptacji ryzyka oraz metodyki przeprowadzania analizy wykorzystane zostały zalecenia organu nadzorczego¹.

Dla potrzeb niniejszej analizy przyjmuje się następującą skalę oceny prawdopodobieństwa i skutku. Jednostka może przyjąć inną skalę, jeżeli jest ona zgodna z przyjętą u administratora metodyką zarządzania ryzykiem.

Wartość	Prawdopodobieństwo	Skutek dla praw i wolności osób
1	Mало prawdopodobne	Niski wpływ; możliwe łatwe usunięcie skutków zdarzenia.
2	Możliwe	Odczuwalny wpływ; konieczne działania korygujące lub wyjaśniające.
3	Prawdopodobne	Istotny wpływ; możliwa skarga, naruszenie poufności lub szkoda dla osoby, której dane dotyczą.

Kryteria akceptacji ryzyka:

Poziom	Wynik
Niski	1-2
Średni	3-4
Wysoki	6-9

Postępowanie

Ryzyko zasadniczo akceptowalne; wystarczający zwykły nadzór.

Ryzyko wymaga monitorowania i okresowej weryfikacji skuteczności zabezpieczeń.

Ryzyko wymaga dodatkowych działań ograniczających albo udokumentowanej decyzji administratora.

Po zastosowaniu środków ograniczających ryzyko jednostka powinna ocenić ryzyko rezidualne, tj. poziom ryzyka pozostający po wdrożeniu zabezpieczeń, oraz wskazać, czy jest ono akceptowalne.

PRAWDOPODOBIENSTWO					
Prawie pewne	SKUTEK				
	1	2	3	4	5
	1	2	3	4	5
	3	4	5	6	7
	5	6	7	8	9
Prawdopodobne	4	5	6	7	8
Możliwe	3	4	5	6	7
Mало prawdopodobne	2	3	4	5	6
Rzadkie	1	2	3	4	5

Poziom ryzyka	Opis działania
Wysoki (W)	Poziom ryzyka akceptowany – działania podejmowane w zależności od wymaganych nakładów
Średni (Ś)	Poziom ryzyka nieakceptowany – działanie może zostać przesunięte w czasie, ale wymaga okresowego monitorowania
Wysoki (W)	Poziom ryzyka nieakceptowany – działanie może zostać przesunięte w czasie, ale wymaga stałego monitorowania
Korygujący (K)	Poziom ryzyka nietolerowany – wymaga natychmiastowego działania

¹ Urząd Ochrony Danych Osobowych, Jak rozumieć podejście oparte na ryzyku? Poradnik RODO Podejście oparte na ryzyku. Część 1, Warszawa 2018; Urząd Ochrony Danych Osobowych, Jak stosować podejście oparte na ryzyku? Poradnik RODO. Podejście oparte na ryzyku. Część 2, Warszawa 2018.

5. Identyfikacja, analiza i ocena ryzyka

Tabela zawiera przykładowe ryzyka związane z publikacją i aktualizacją informacji w CRU. Jednostka powinna uzupełnić ją o własne ryzyka wynikające z lokalnego obiegu umów, struktury organizacyjnej, liczby osób upoważnionych, narzędzi informatycznych oraz przyjętych procedur.

Zagrożenie - źródło ryzyka	Zagrożony atrybut danych	Skutek	Praw dop.	Sku tek	Ryzyko pierwotne	Środki techniczne i organizacyjne ograniczające ryzyko	Ryzyko rezydualne	Akceptacja / działania dodatkowe
Dostęp osób nieuprawnionych do konta w systemie CRU	integralność danych	/	1	2	niski	Zabezpieczenie dostępu do konta w systemie poprzez wymóg autoryzacji użytkownika, indywidualne konta, okresowy przegląd uprawnień, stosowanie zabezpieczeń sieci roboczych	niski	Akceptowalne, monitorować zmiany kadrowe i odbieranie uprawnień po ustaniu obowiązków
Nieprawidłowa integralność danych	integralność danych	/	3	2	średni	Udostępnienie w CRU danych, które nie powinny być udostępnione	średni	Wymaga okresowego monitorowania, wskazać osobę odpowiedzialną za weryfikację i termin przeglądu
Ujawnienie nadmiarowych, np. PESEL, adresów, danych kontaktowych, numeru dokumentu lub danych z dokumentów źródłowych	integralność danych	/	3	3	wysoki	Nieuprawnione ujawnienie danych, które nie są wymagane do publikacji w CRU; możliwość skargi, naruszenia prywatności lub konieczność zgłoszenia naruszenia	średni	Wymaga wdrożenia checklisty i stałego monitorowania, uzupełnić termin, właściciela działania i sposób dokumentowania weryfikacji
Wprowadzenie błędnych danych osobowych	integralność danych	/	3	2	średni	Udostępnianie w CRU danych nieprawidłowych	średni / niski	Akceptowalne pod warunkiem prowadzenia przeglądów, uzupełnić częstotliwość przeglądu
Brak realizacji uprawnień osób, której dane dotyczą	integralność danych	/	3	3	wysoki	Niedopodinięcie obowiązku realizacji uprawnień osób; utrzymywanie w CRU danych nieprawidłowych	średni	Wymaga stałego monitorowania, każde żądanie powinno być odnotowane i przekazane do IOD lub osoby odpowiedzialnej
Nieusunięcie nieprawidłowych danych po upływie terminu lub po stwierdzeniu nieprawidłowości	integralność danych	/	3	2	średni	Udostępnianie w CRU danych osobowych, które nie powinny już być dostępne albo powinny zostać skorygowane	średni / niski	Akceptowalne pod warunkiem cyklicznych przeglądów; uzupełnić termin i osobę odpowiedzialną
Brak okresowego przeglądu uprawnień użytkowników CRU	integralność danych	/	2	2	średni	Ryzyko utrzymania dostępu przez osoby, które nie wykonują już zadań związanych z CRU	niski	Akceptowalne po wdrożeniu przeglądów; rekomendowany przegląd co najmniej raz na 6 miesięcy albo po każdej zmianie organizacyjnej

Należy dokonać analizy ryzyka z uwzględnieniem indywidualnych uwarunkowań przetwarzania danych osobowych w danej jednostce organizacyjnej. Należy zweryfikować, czy wskazane zabezpieczenia są rzeczywiście stosowane oraz czy ryzyko rezydualne jest akceptowalne dla administratora.

6. Postępowanie z ryzykiem

Ze względu na zakres danych osobowych podlegających udostępnieniu w CRU, przy uwzględnieniu zasady minimalizacji danych oraz obowiązku publikowania wyłącznie informacji wymaganych przepisami, przyjmuje się, że część analizowanych ryzyk może być ograniczona do poziomu akceptowalnego po zastosowaniu wskazanych środków technicznych i organizacyjnych. Jednostka powinna jednak samodzielnie zweryfikować poziom ryzyka rezydualnego, w szczególności w zakresie ryzyka publikacji danych nadmiarowych, błędnych lub niepodlegających udostępnieniu. W celu zminimalizowania ryzyka w jednostce przyjęto / planuje się przyjąć dokument: Procedura ochrony danych osobowych przy prowadzeniu CRU albo inny równoważny dokument regulujący zasady weryfikacji i publikacji danych w CRU.

W zakresie ryzyka ujawnienia danych nadmiarowych za kluczowe uznaje się stosowanie zasady minimalizacji danych, weryfikację wpisu przed publikacją, anonimizację albo usuwanie danych niewymaganych do publikacji oraz dokumentowanie przypadków, w których publikacja określonych informacji została ograniczona ze względu na przepisy o ochronie danych osobowych lub ograniczenia prawa do informacji publicznej.

W zakresie ryzyka dostępu osób nieuprawnionych do konta w systemie CRU podjęte środki w postaci zabezpieczenia dostępu do konta poprzez wymóg autoryzacji użytkownika oraz stosowania zapor typu firewall sprawiają, że ryzyko zostało ograniczone do poziomu akceptowalnego.

W zakresie ryzyka dokonania nieprawidłowej oceny dopuszczalności udostępnienia danych w CRU, określono procedurę ochrony danych osobowych przy prowadzeniu CRU oraz przyjęto wymóg weryfikacji danych osobowych wprowadzanych do CRU. Ponadto planowane jest przeprowadzenie

szkolenia pracowników z zakresu udostępniania informacji w CRU. Przyjęte zabezpieczenia pozwalają uznać, że ryzyko zostało ograniczone, jednak poziom ryzyka sprawia, że działania wymagają okresowego monitorowania.

W zakresie ryzyka wprowadzenie do CRU błędnych danych osobowych, określono procedurę ochrony danych osobowych przy prowadzeniu CRU, przyjęto wymóg weryfikacji danych osobowych wprowadzanych do CRU, za konieczne uznano również dokonywanie okresowych przeglądów danych udostępnianych w CRU oraz korygowanie danych nieprawidłowych. Przyjęte zabezpieczenia pozwalają uznać, że ryzyko zostało ograniczone, jednak poziom ryzyka sprawia, że działania wymagają okresowego monitorowania.

W zakresie ryzyka braku realizacji uprawnionych żądań osoby, której dane dotyczą określono procedurę ochrony danych osobowych przy prowadzeniu CRU, uznano za niezbędne monitorowanie przez inspektora ochrony danych realizacji uprawnień osób, których dane dotyczą. Przyjęte zabezpieczenia pozwalają ograniczyć ryzyko, jednak o każdym przypadku żądania podmiotu danych powinien być informowany inspektor ochrony danych, który powinien wspierać administratora w realizacji tych żądań. W szczególności brak realizacji uprawnień informacyjnych i korekcyjnych może pociągać za sobą duże ryzyko naruszenia praw osób, których dane poddawane są przetwarzaniu, co sprawia, że działania wymagają stałego monitorowania.

W zakresie ryzyka nieusunięcia z CRU danych po upływie terminu ich udostępniania przyjęto zabezpieczenia w postaci określenia procedury ochrony danych osobowych przy prowadzeniu CRU, przewidziano również dokonywanie okresowych przeglądów danych udostępnianych w CRU, a także wymóg usuwania danych w kontekście korygowania danych.

7. Decyzja administratora i zatwierdzenie analizy

Po przeprowadzeniu analizy ryzyka administrator uznaje, że ryzyka związane z przetwarzaniem danych osobowych w ramach realizacji obowiązków dotyczących CRU JSFP zostały zidentyfikowane, ocenione oraz ograniczone przez wskazane środki techniczne i organizacyjne.

Ryzyka rezydualne uznaje się za: akceptowalne.

Wynik analizy	Akceptowalne
Działania dodatkowe do wykonania	-----
Osoba odpowiedzialna za działania dodatkowe	-----
Termin wykonania / przeglądu	30.06.2026
Podpis osoby zatwierdzającej	<i>Barbara Ścisł</i> [data i podpis]

8. Minimalna checklista przed przyjęciem dokumentu w jednostce

Lp.	Czynność do potwierdzenia
1	uzupełniono metrykę dokumentu i dane jednostki;
2	zweryfikowano lokalny obieg umów oraz osoby odpowiedzialne za publikację i kontrolę danych w CRU;
3	wskazano zabezpieczenia faktycznie stosowane w jednostce;
4	sprawdzone, czy w jednostce przyjęto procedurę / instrukcję dotyczącą CRU albo czy należy ją przyjąć;
5	zweryfikowano zakres danych publikowanych w CRU pod kątem minimalizacji danych;
6	określono sposób anonimizacji lub usuwania danych nadmiarowych z dokumentów źródłowych;
7	oceniono ryzyko rezydualne i wskazano, czy jest akceptowalne;
8	ustalono częstotliwość przeglądów wpisów w CRU i uprawnień użytkowników.

Analiza ryzyka dla przetwarzania danych osobowych w Centralnym Rejestrze Umów dla Ośrodka Pomocy Społecznej w Niemcach

Metryka dokumentu - do uzupełnienia przez jednostkę

Nazwa jednostki	Ośrodek Pomocy Społecznej
Administrator danych	Ośrodek Pomocy Społecznej
Komórka odpowiedzialna za CRU	Dział organizacyjny- administracyjny
Właściciel procesu / koordynator CRU	Ośrodek Pomocy Społecznej
Inspektor ochrony danych	Natalia Pietruszka
Osoby / stanowiska upoważnione do pracy w Starszy inspektor Elżbieta Kroczy; referent Sylwia Gziut	
CRU	
Data sporządzenia / aktualizacji analizy	30.06.2026
Wersja dokumentu	1
Osoba sporządzająca	Natalia Pietruszka
Osoba zatwierdzająca	Kierownik Ośrodka Pomocy Społecznej Barbara Ścisiel
Data kolejnego przeglądu	30.06.2027

1. Ustalenie kontekstu przetwarzania danych

Zgodnie z art. 34a ust. 1 Ustawy z 27.08.2009 r. o finansach publicznych (Dz.U. z 2025 r., poz. 1483 ze zm. – dalej: u.f.p.), kierownik jednostki sektora finansów publicznych ma obowiązek udostępniania i aktualizowania w Centralnym Rejestrze Umów Jednostek Sektora Finansów Publicznych (dalej: CRU) informacji o umowach zawartych przez jednostkę sektora finansów publicznych (dalej: j.s.f.p.) lub na jej rzecz. Realizacja tego obowiązku wymaga przetwarzania danych osobowych, dlatego w niniejszym dokumencie przeprowadzona zostanie analiza ryzyka naruszenia praw i wolności osób, których dane dotyczą związanego z przetwarzaniem danych osobowych, zgodnie z art. 24 i art. 32 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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 (Dz. Urz. UE. L. z 2016 r., poz. 119) – dalej: ogólne rozporządzenie o ochronie danych.

Informacje o umowach, w tym dane osobowe, będą wprowadzane do systemu teleinformatycznego CRU przez osoby upoważnione przez kierownika j.s.f.p. Analiza ryzyka dotyczyć będzie przetwarzania danych osobowych w zakresie informacji o umowach zamieszczanych w CRU w imieniu kierownika jednostki. Dane osobowe udostępniane w CRU są gromadzone w Ośrodku Pomocy Społecznej, pochodzą z umów zawieranych przez jednostkę z kontrahentami (wykonawcami umów).

W zakresie zapewnienia funkcjonowania systemu teleinformatycznego, w którym jest prowadzony CRU, administratorem danych użytkowników kont w systemie oraz innych danych w zakresie, w jakim jest to niezbędne do zapewnienia funkcjonowania systemu jest Minister Finansów, który ma obowiązek przeprowadzenia analizy ryzyka i przyjęcia odpowiednich zabezpieczeń, dlatego ten obszar przetwarzania danych nie będzie objęty niniejszą analizą.

2. Opis przetwarzanych danych i ich klasyfikacja

W CRU udostępniane będą dane osobowe osoby, z jaką Ośrodek Pomocy Społecznej w Niemcach zawarła umowę odpłatną zawieraną między zamawiającym a wykonawcą, której przedmiotem jest nabycie przez zamawiającego od wybranego wykonawcy robót budowlanych, dostaw lub usług oraz która została zawarta w formie pisemnej, dokumentowej, elektronicznej albo innej formie szczególnej, bez względu na wartość przedmiotu umowy, z wyjątkami odnoszącymi się do umów określonych w art. 34a ust. 5 u.f.p., w tym m.in. umów z zakresu prawa pracy. W CRU nie udostępnia się informacji o umowie, co do których prawo do informacji publicznej podlega ograniczeniu na podstawie art. 5 ust. 1 i 2-2b ustawy z 6.09. 2001 r. o dostępie do informacji publicznej (Dz.U. z 2022 r. poz. 902, dalej u.d.i.p.). CRU jest jawny, prowadzony w systemie teleinformatycznym i umożliwia wyszukiwanie informacji o umowie udostępnionych w CRU oraz wgląd do tych informacji.

Do danych osobowych, które będą udostępniane w CRU należą informacje o osobach fizycznych z którymi zawarte zostały umowy finansowane ze środków publicznych. (np. dane osoby fizycznej, z którą gmina zawarła umowę zlecenia). Przepis art. 34a ust. 7 u.f.p. wśród informacji podlegających udostępnianiu wskazuje „oznaczenie stron umowy” (pkt 4). Zgodnie z §3 pkt 2 rozporządzenia Ministra Finansów i Gospodarki z 30.03.2026 r. w sprawie Centralnego Rejestru Umów Jednostek Sektora Finansów Publicznych (Dz.U. z 2026 r., poz. 440, dalej: rozporządzenie CRU), oznaczenie stron umowy obejmuje a) nazwę (firmę), numer REGON, numer identyfikacji podatkowej (NIP), jeżeli został zamieszczony w bazie REGON, i adres siedziby albo adres wykonywania działalności gospodarczej - w przypadku gdy stroną umowy jest j.s.f.p. lub przedsiębiorca z siedzibą albo miejscem wykonywania działalności poza terytorium RP; c) imię i nazwisko - w przypadku gdy stroną umowy jest j.s.f.p. lub przedsiębiorca z siedzibą albo miejscem wykonywania działalności poza terytorium RP; c) imię i nazwisko - w przypadku gdy stroną umowy jest osoba fizyczna. W CRU wpisywane będą zarówno informacje identyfikujące przedsiębiorców, w tym osób fizycznych prowadzących działalność gospodarczą, jak też informacje o osobach fizycznych, które działalności gospodarczej nie prowadzą, a z którymi zawarta została umowa. W przypadku przedsiębiorców będących osobami fizycznymi zakres danych osobowych jest szerszy i obejmuje ich firmę oraz adres, natomiast w odniesieniu do osób fizycznych, nieprowadzących działalności gospodarczej, zakres informacji udostępnianych w CRU jest wąski i zawiera jedynie imię i nazwisko, natomiast nie powinno się publikować innych danych (w szczególności numerów PESEL, adresów zamieszkania, czy też innych danych osobowych, które są zawarte w umowach).

Z realizacją obowiązku udostępniania i aktualizacji informacji w CRU wiąże się także przetwarzanie danych osobowych kierownika jednostki oraz osób przez niego upoważnionych. Zakres danych tych osób obejmuje imię i nazwisko oraz stanowisko służbowe. Jednak w zakresie przetwarzania danych tych osób w systemie teleinformatycznym CRU administratorem jest właściwy minister, do którego obowiązków należy przeprowadzenie analizy ryzyka przetwarzania tego rodzaju danych osobowych.

Dane osobowe będą wprowadzane do CRU za pośrednictwem komputerów w jednostce, z wykorzystaniem oprogramowania i kont dostępowych udostępnianych przez administratora systemu teleinformatycznego CRU. Na administratorze systemu ciąży obowiązek odpowiedniego zabezpieczenia systemu i oprogramowania w zakresie ochrony integralności oraz dostępności danych przetwarzanych w systemie. Informacje prawidłowo udostępnione w CRU mają charakter jawny, jednak do czasu ich publikacji, a także w zakresie danych źródłowych, danych nadmiarowych, dokumentów roboczych, upoważnień, danych kont użytkowników oraz danych niepodlegających udostępnieniu, jednostka zapewnia ich poufność, integralność i dostępność zgodnie z art. 32 RODO.

3. Opis stosowanych zabezpieczeń

Z przetwarzaniem danych osobowych w CRU może wiązać się ryzyko wynikające w szczególności z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych, Stosownie do zagrożeń podjęte zostały odpowiednie środki mające na celu ograniczenie ryzyka.

Dane osobowe przetwarzane w związku z realizacją obowiązku udostępniania informacji w CRU są zabezpieczone z wykorzystaniem następujących rodzajów zabezpieczeń:

- zabezpieczenia organizacyjne – przyjęta została Procedura ochrony danych osobowych przy prowadzeniu CRU, upoważnione do pobierania kluczy do pomieszczeń, w których przetwarza się dane są jedynie osoby uprawnione;
- zabezpieczenia osobowe – uprawnienia do pracy w systemie CRU nadawane są wybranym pracownikom, dokonywana jest weryfikacja tych uprawnień, nadawane są upoważnienia do przetwarzania danych osobowych;
- zabezpieczenia techniczne - programowe: dostęp do systemu CRU przyznawany jest jedynie uprawnionym użytkownikom i wymaga uwierzytelnienia; komputery wyposażone są w oprogramowanie typu firewall oraz oprogramowanie antywirusowe, programy są na bieżąco aktualizowane;
- zabezpieczenia techniczne – fizyczne: dostęp do pomieszczeń w których przetwarzane są dane jest ograniczony, pomieszczenia są zamknięte, papierowe nośniki, z których dane wprowadzane są do systemu CRU są przechowywane w zamkniętych szafach.

4. Określenie kryteriów akceptacji ryzyka

Poziom ryzyka to iloczyn prawdopodobieństwa zdarzenia i jego skutku. W niniejszej analizie ryzyka w zakresie określenia kryteriów akceptacji ryzyka oraz metodyki przeprowadzania analizy wykorzystane zostały zalecenia organu nadzorczego¹.

Dla potrzeb niniejszej analizy przyjmuje się następującą skalę oceny prawdopodobieństwa i skutku. Jednostka może przyjąć inną skalę, jeżeli jest ona zgodna z przyjętą u administratora metodyką zarządzania ryzykiem.

Wartość		Prawdopodobieństwo		Skutek dla praw i wolności osób	
1	Kryteria akceptacji ryzyka:	1	Mato prawdopodobne	Niski wpływ, możliwe łatwe usunięcie skutków zdarzenia.	
2		2	Mozliwe	Odczuwalny wpływ, konieczne działania korygujące lub wyjaśniające.	
3		3	Prawdopodobne	Istotny wpływ, możliwa skarga, naruszenie poufności lub szkoda dla osoby, której dane dotyczą.	

Poziom	Wynik	Postępowanie
Niski	1-2	Ryzyko zasadniczo akceptowalne, wystarczający zwykły nadzór.
Średni	3-4	Ryzyko wymaga monitorowania i okresowej weryfikacji skuteczności zabezpieczeń.
Wysoki	6-9	Ryzyko wymaga dodatkowych działań ograniczających albo udokumentowanej decyzji administratora.

Po zastosowaniu środków ograniczających ryzyko jednostka powinna ocenić ryzyko rezidualne, tj. poziom ryzyka pozostający po wdrożeniu zabezpieczeń, oraz wskazać, czy jest ono akceptowalne.

PRAWDOPODOBIENSTWO		SKUTEK				
		Bardzo niski	Niski	Średni	Wysoki	Bardzo wysoki
Prawie pewne	5	Ś	W	K	K	K
Prawdopodobne	4	Ś	W	W	K	K
Mozliwe	3	Ś	Ś	W	W	K
Mato prawdopodobne	2	Ś	Ś	Ś	W	W
Rzadkie	1	Ś	Ś	Ś	W	W

Poziom ryzyka	Opis działania
Niski (N)	Poziom ryzyka akceptowany – działania podejmowane w zależności od wymaganych nakładów
Średni (Ś)	Poziom ryzyka nieakceptowany – działanie może zostać przesunięte w czasie, ale wymaga okresowego monitorowania
Wysoki (W)	Poziom ryzyka nieakceptowany – działanie może zostać przesunięte w czasie, ale wymaga stałego monitorowania
Korygujący (K)	Poziom ryzyka nietolerowany – wymaga natychmiastowego działania

¹ Urząd Ochrony Danych Osobowych, Jak rozumieć podejście oparte na ryzyku? Poradnik RODO Podejście oparte na ryzyku. Część 1, Warszawa 2018; Urząd Ochrony Danych Osobowych, Jak stosować podejście oparte na ryzyku? Poradnik RODO. Podejście oparte na ryzyku. Część 2, Warszawa 2018.

5. Identyfikacja, analiza i ocena ryzyka

Tabela zawiera przykładowe ryzyka związane z publikacją i aktualizacją informacji w CRU. Jednostka powinna uzupełnić ją o własne ryzyka wynikające z lokalnego obiegu umów, struktury organizacyjnej, liczby osób upoważnionych, narzędzi informatycznych oraz przyjętych procedur:

Zagrożenie - źródło ryzyka	Zagrożony atrybut danych	Skutek	Praw dop.	Sku	Ryzyko pierwotne	Środki techniczne i organizacyjne ograniczające ryzyko	Ryzyko rezydualne	Akceptacja / działania dodatkowe
Dostęp osób nieuprawnionych do konta w systemie CRU	integralność danych	/	1	2	niski	Zabezpieczenie dostępu do konta w systemie poprzez wymóg autoryzacji użytkownika; indywidualne konta; okresowy przegląd uprawnień; stosowanie zabezpieczeń sieci roboczych.	niski	Akceptowalne; monitorować zmiany kadrowe i odbieranie uprawnień po ustaniu obowiązków
Nieprawidłowa dopuszczalność udostępnienia danych	integralność danych	/	3	2	średni	Udostępnienie w CRU danych, które nie powinny być udostępniane	średni	Wymaga okresowego monitorowania; wskazać osobę odpowiedzialną za weryfikację i termin przeglądu.
Ujawnienie nadmiarowych, np. PESEL, adresów zamieszkania, prywatnych danych kontaktowych, numeru dokumentu lub danych z dokumentów źródłowych	integralność danych	/	3	3	wysoki	Nieuprawnione ujawnienie danych, które nie są wymagane do publikacji w CRU; możliwość skargi, naruszenia prywatności lub konieczność zgłoszenia naruszenia.	średni	Wymaga wdrożenia checklisty i stałego monitorowania; uzupełnić termin, właściciela działania i sposób dokumentowania weryfikacji.
Wprowadzenie do CRU błędnych danych osobowych	integralność danych	/	3	2	średni	Udostępnianie w CRU danych nieprawidłowych danych osobowych albo danych zawierających błędy	średni / niski	Akceptowalne pod warunkiem prowadzenia przeglądów; uzupełnić częstotliwość przeglądu
Brak realizacji uprawnień	integralność danych	/	3	3	wysoki	Niedostarczenie informacji lub brak realizacji uprawnień osobą, utrzymywanie w CRU danych nieprawidłowych	średni	Wymaga stałego monitorowania; każde żądanie powinno być odnotowane i przekazane do IOD lub osoby odpowiedzialnej
Nieusunięcie nadmiarowych danych po upływie terminu lub po stwierdzeniu nieprawidłowości	integralność danych	/	3	2	średni	Udostępnianie w CRU danych osobowych, które nie powinny już być dostępne albo powinny zostać skorygowane	średni / niski	Akceptowalne pod warunkiem cyklicznych przeglądów; uzupełnić termin i osobę odpowiedzialną
Brak okresowego przeglądu uprawnień użytkowników CRU	integralność danych	/	2	2	średni	Ryzyko utrzymania dostępu przez osoby, które nie wykonują już zadań związanych z CRU	niski	Akceptowalne po wdrożeniu przeglądów; rekomendowany przegląd co najmniej raz na 6 miesięcy albo po każdej zmianie organizacyjnej

Należy dokonać analizy ryzyka z uwzględnieniem indywidualnych uwarunkowań przetwarzania danych osobowych w danej jednostce organizacyjnej. Należy zweryfikować, czy wskazane zabezpieczenia są rzeczywiście stosowane oraz czy ryzyko rezydualne jest akceptowalne dla administratora.

6. Postępowanie z ryzykiem

Ze względu na zakres danych osobowych podlegających udostępnianiu w CRU, przy uwzględnieniu zasady minimalizacji danych oraz obowiązku publikowania wyłącznie informacji wymaganych przepisami, przyjmuje się, że część analizowanych ryzyk może być ograniczona do poziomu akceptowalnego po zastosowaniu wskazanych środków technicznych i organizacyjnych. Jednostka powinna jednak samodzielnie zweryfikować poziom ryzyka rezydualnego, w szczególności w zakresie ryzyka publikacji danych nadmiarowych, błędnych lub niepodlegających udostępnieniu. W celu zminimalizowania ryzyka w jednostce przyjęto / planuje się przyjęcie dokument: Procedura ochrony danych osobowych przy prowadzeniu CRU albo inny równoważny dokument regulujący zasady weryfikacji i publikacji danych w CRU.

W zakresie ryzyka ujawnienia danych nadmiarowych za kluczowe uznaje się stosowanie zasady minimalizacji danych, weryfikację wpisu przed publikacją, anonimizację albo usuwanie danych niewymaganych do publikacji oraz dokumentowanie przypadków, w których publikacja określonych informacji została ograniczona ze względu na przepisy o ochronie danych osobowych lub ograniczenia prawa do informacji publicznej.

W zakresie ryzyka dostępu osób nieuprawnionych do konta w systemie CRU podjęte środki w postaci zabezpieczenia dostępu do konta poprzez wymóg autoryzacji użytkownika oraz stosowania zapory typu firewall sprawiają, że ryzyko zostało ograniczone do poziomu akceptowalnego.

W zakresie ryzyka dokonania nieprawidłowej oceny dopuszczalności udostępnienia danych w CRU, określono procedurę ochrony danych osobowych przy prowadzeniu CRU oraz przyjęto wymóg weryfikacji danych osobowych wprowadzanych do CRU. Ponadto planowane jest przeprowadzenie

szkolenia pracowników z zakresu udostępniania informacji w CRU. Przyjęte zabezpieczenia pozwalają uznać, że ryzyko zostało ograniczone, jednak poziom ryzyka sprawia, że działania wymagają okresowego monitorowania.

W zakresie ryzyka wprowadzenie do CRU błędnych danych osobowych, określono procedurę ochrony danych osobowych przy prowadzeniu CRU, przyjęto wymóg weryfikacji danych osobowych wprowadzanych do CRU, za konieczne uznano również dokonywanie okresowych przeglądów danych udostępnianych w CRU oraz korygowanie danych nieprawidłowych. Przyjęte zabezpieczenia pozwalają uznać, że ryzyko zostało ograniczone, jednak poziom ryzyka sprawia, że działania wymagają okresowego monitorowania.

W zakresie ryzyka braku realizacji uprawnień żądań osoby, której dane dotyczą określono procedurę ochrony danych osobowych przy prowadzeniu CRU, uznano za niezbędne monitorowanie przez inspektora ochrony danych realizacji uprawnień osób, których dane dotyczą. Przyjęte zabezpieczenia pozwalają ograniczyć ryzyko, jednak o każdym przypadku żądania podmiotu danych powinien być informowany inspektor ochrony danych, który powinien wspierać administratora w realizacji tych żądań. W szczególności brak realizacji uprawnień informacyjnych i korekcyjnych może pociągać za sobą duże ryzyko naruszenia praw osób, których dane poddawane są przetwarzaniu, co sprawia, że działania wymagają stałego monitorowania.

W zakresie ryzyka nieusunięcia z CRU danych po upływie terminu ich udostępniania przyjęto zabezpieczenia w postaci określenia procedury ochrony danych osobowych przy prowadzeniu CRU, przewidziano również dokonywanie okresowych przeglądów danych udostępnianych w CRU, a także wymóg usuwania danych w kontekście korygowania danych.

7. Decyzja administratora i zatwierdzenie analizy

Po przeprowadzeniu analizy ryzyka administrator uznaje, że ryzyka związane z przetwarzaniem danych osobowych w ramach realizacji obowiązków dotyczących CRU JSFP zostały zidentyfikowane, ocenione oraz ograniczone przez wskazane środki techniczne i organizacyjne.

Ryzyka rezydualne uznaje się za: akceptowalne.

Wynik analizy	Akceptowalne
Działania dodatkowe do wykonania	-----
Osoba odpowiedzialna za działania dodatkowe	-----
Termin wykonania / przeglądu	30.06.2026
Podpis osoby zatwierdzającej	<i>Barbara Ścisiel</i>
	[data i podpis]

8. Minimalna checklista przed przyjęciem dokumentu w jednostce

Lp.	Czynność do potwierdzenia
1	uzupełniono metrykę dokumentu i dane jednostki;
2	zweryfikowano lokalny obieg umów oraz osoby odpowiedzialne za publikację i kontrolę danych w CRU;
3	wskazano zabezpieczenia faktycznie stosowane w jednostce;
4	sprawdzone, czy w jednostce przyjęto procedurę / instrukcję dotyczącą CRU albo czy należy ją przyjąć;
5	zweryfikowano zakres danych publikowanych w CRU pod kątem minimalizacji danych;
6	określono sposób anonimizacji lub usuwania danych nadmiarowych z dokumentów źródłowych;
7	oceniono ryzyko rezydualne i wskazano, czy jest akceptowalne;
8	ustalono częstotliwość przeglądów wpisów w CRU i uprawnień użytkowników.

KIEROWNIK
Ośrodka Pomocy Społecznej
w Niepazach
mgr Barbara Ścisiel