INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM REJESTR NALEŻNOŚCI PUBLICZNOPRAWNYCH

MINISTERSTWO FINANSÓW						
Nazwa	**INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM REJESTR NALEŻNOŚCI PUBLICZNOPRAWNYCH**					
Krótki opis dokumentu	Dokument określa metody, środki i procedury zarządzania systemem Rejestr Należności Publicznoprawnych					
Właściciel dokumentu	Izba Administracji Skarbowej w Szczecinie - Wydział Rejestru Należności Publicznoprawnych oraz Nadzoru nad Rejestracją i Centrum Organu Wierzyciela					
Opracowany przez	Nazwa komórki organizacyjnej	Izba Administracji Skarbowej w Szczecinie - Wydział Rejestru Należności Publicznoprawnych oraz Nadzoru nad Rejestracją i Centrum Organu Wierzyciela				
Akceptacja w zakresie przepisów uodo **Wieloosobowe Stanowisko Ochrony Danych (IWD)**	Imię i nazwisko, stanowisko	Andrzej Żurawski Inspektor Ochrony Danych	Data	02.04 2019 r	Podpis	
Akceptacja w zakresie zabezpieczeń technicznych **Dział Bezpieczeństwa i Ochrony Informacji (IWO)**	Imię i nazwisko, stanowisko	Kierownik Działu Eugeniusz Pietrzak	Data	3.04. 2019 r	Podpis	
Akceptacja w zakresie zabezpieczeń technicznych **Pion Informatyki (IZPI)**	Imię i nazwisko, stanowisko	Z-ca Dyrektora Izby Administracji Skarbowej w Szczecinie Damian Garczyński	Data	2.04 2019	Podpis	
Akceptacja w zakresie merytorycznym (biznesowym) **Pion Poboru i Egzekucji (IZPE)**	Imię i nazwisko, stanowisko	Z up. Dyrektora Izby Administracji Skarbowej w Szczecinie Robert Hołubasz Zastępca Dyrektora Izby Administracji Skarbowej w Szczecinie	Data	03.04 2019	Podpis	
Zatwierdził	Imię i nazwisko, stanowisko	wz. Sylwia Jarosławska Zastępca Dyrektora	Data	05.04 2019	Podpis	

SPIS TREŚCI

1 WYKAZ SKRÓTÓW I TERMINÓW

1)	**ADO**	Administrator Danych Osobowych – Dyrektor Izby Administracji Skarbowej w Szczecinie
2)	**ASI**	Administrator Systemu Informatycznego
3)	**CIRF**	Centrum Informatyczne Resortu Finansów
4)	**DIAS**	Dyrektorzy Izb Administracji Skarbowej
5)	**IAS**	Izba Administracji Skarbowej
6)	**Incydent związany z bezpieczeństwem przetwarzania danych osobowych**	Pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.
7)	**IOD**	Inspektor Ochrony Danych
8)	**IZSI RNP**	Instrukcja Zarządzania Systemem Informatycznym RNP
9)	**Jednostka organizacyjna**	komórki organizacyjne, izby administracji skarbowej, urzędy skarbowe
10)	**JST**	Jednostki samorządu terytorialnego
11)	**KAS**	Krajowa Administracja Skarbowa
12)	**LADO**	Lokalny Administrator Danych Osobowych
13)	**NUS**	Naczelnicy Urzędów Skarbowych
14)	**Organ RNP**	Organ prowadzący rejestr (RNP) - Dyrektor Izby Administracji Skarbowej w Szczecinie
15)	**Podmiot uprawniony**	Podmioty wymienione w art. 18q § 2 ustawy z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz. U. z 2018 r., poz. 1314 z późn. zm.)
16)	**pracownik**	Funkcjonariusz, pracownik, stażysta, praktykant, wolontariusz, pracownik zleceniowy.
17)	**RNP**	Rejestr Należności Publicznoprawnych
18)	**RODO**	Rozporządzenie nr 2016/679 Parlamentu Europejskiego i Rady (UE) 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)
19)	**u.p.e.a**	Ustawa z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz. U. z 2018 r., poz. 1314 z późn. zm.)
20)	**US**	Urząd skarbowy
21)	**Użytkownik**	pracownik przetwarzający dane w RNP zatrudniony przez ADO, wierzyciela lub podmiot uprawniony
22)	**Wierzyciel**	Jednostka samorządu terytorialnego lub naczelnik urzędu skarbowego
23)	**Zobowiązany**	Jest to osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej albo osoba fizyczna, która nie wykonała w terminie obowiązku o charakterze pieniężnym, dla której wierzycielem jest NUS lub JST.

2 CEL DOKUMENTU

Celem opracowania Instrukcji Zarządzania Systemem Informatycznym Rejestr Należności Publicznoprawnych jest określenie zasad prawidłowej eksploatacji systemu z zapewnieniem ochrony danych osobowych przed ich udostępnieniem osobom nieuprawnionym, zmianą, utratą, uszkodzeniem lub zniszczeniem tych danych oraz ich przetwarzanie z naruszeniem przepisów o ochronie danych osobowych. Ochronie podlega również infrastruktura serwerowa, sprzęt komputerowy, systemy operacyjne

i informatyczne wykorzystywane do pracy z systemem oraz pomieszczenia, w których odbywa się proces przetwarzania danych systemu RNP.

3 ODPOWIEDZIALNOŚĆ

Dokument jest dedykowany wszystkim osobom i podmiotom odpowiedzialnym za prawidłowe funkcjonowanie Rejestru Należności Publicznoprawnych oraz za jego eksploatację (DIAS, NUS, CIRF, JST, podmioty uprawnione, które uzyskały uprawnienia dostępowe do RNP).

3.1 PODMIOTY ODPOWIEDZIALNE ZA EKSPLOATACJĘ SYSTEMU ORAZ JEGO PRAWIDŁOWE WYKORZYSTANIE

NAZWA PODMIOTU	OPIS ZAKRESU ODPOWIEDZIALNOŚCI
Adminstrator Danych Osobowych (ADO) / Właściciel systemu	Na podstawie rozporządzenia Ministra Finansów z dnia 30 maja 2018 r. w sprawie wyznaczenia organu Krajowej Administracji Skarbowej do prowadzenia Rejestru Należności Publicznoprawnych (Dz. U. 2018 r., poz. 1123) organem wyznaczonym do prowadzenia Rejestru Należności Publicznoprawnych jest Dyrektor Izby Administracji Skarbowej w Szczecinie. Realizuje on zadania wynikające z art. 24 RODO a także wynikające z u.p.e.a. oraz RMF
Lokalny Adminstrator Danych Osobowych (LADO)	Lokalny Administrator Danych Osobowych to organ/podmiot realizujący zadania ADO w jednostkach podmiotów uprawnionych, który nadzoruje bezpieczeństwo przetwarzania danych osobowych w swojej jednostce.
Inspektor Ochrony Danych (IOD)	Osoba odpowiedzialna za monitorowanie prawidłowości przetwarzaniem danych osobowych. Szczegółowe zadania Inspektora wynikają bezpośrednio z RODO. Do głównych zadań IOD należy: a) informowanie ADO/LADO, oraz w szczególnych okolicznościach pracowników, którzy przetwarzają dane osobowe, o ich obowiązkach wynikających z przepisów o ochronie danych osobowych, b) monitorowanie przestrzegania przepisów o ochronie danych osobowych, c) udzielanie zaleceń co do oceny skutków dla ochrony danych na wniosek ADO/LADO, d) współpraca z organem nadzorczym oraz pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych, e) pełnienie zadań „punktu kontaktowego” dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem przysługujących im praw.
Organ nadzorczy	Organ nadzorczy oznacza niezależny organ publiczny ustanowiony przez ustawodawstwo krajowe zgodnie z art. 51 RODO. Zadaniem organu nadzorczego jest opiniowanie oraz nadzór nad wdrożeniem środków bezpieczeństwa przez ADO/LADO. Organ nadzorczy jest również adresatem powiadomień o naruszeniu bezpieczeństwa danych osobowych. W ramach posiadanych kompetencji organ nadzorczy jest uprawniony do nakładania kar administracyjnych na ADO/LADO. W Polsce organem nadzorczym jest Prezes Urzędu Ochrony Danych Osobowych.

Administrator Systemu Informatycznego (ASI)	1. Administratorzy merytoryczni są to pracownicy wyznaczonej komórki organizacyjnej IAS w Szczecinie. Są to osoby posiadające wiedzę i umiejętności w zakresie działania RNP. W zakresie obowiązków mają wsparcie wszystkich organizacji w zakresie znajomości funkcjonalności systemu i nadawanie uprawnień administratorom lokalnym. Biorą udział w rozwoju systemu i przekazują na poziom centralny zidentyfikowane ryzyka. 2. Administratorzy lokalni to pracownicy jednostek wierzycieli i podmiotów uprawnionych posiadający uprawnienia do nadawania kolejnych uprawnień dostępowych do danych RNP w obszarze jednostki, w której są zatrudnieni. 3. Administratorzy techniczni to pracownicy CIRF, administrujący systemami informatycznymi, w tym siecią, systemami operacyjnymi, aplikacjami i bazami danych.
Użytkownicy	W celu zapewnienia integralności, poufności i rozliczalności stosuje się niżej wymienione, zasady odpowiedzialności. Za integralność przetwarzanych danych osobowych odpowiedzialny jest: 1) użytkownik, 2) bezpośredni przełożony użytkownika, 3) administrator lokalny, pracownik merytoryczny, którym przypisano uprawnienia konieczne do pracy w systemie, 4) administratorzy techniczni w zakresie zabezpieczenia ruchu sieciowego, spójności baz danych oraz oprogramowania antywirusowego. Za poufność przetwarzanych danych osobowych odpowiedzialni są: 1) wszyscy użytkownicy/pracownicy, 2) bezpośredni przełożony użytkownika w zakresie udostępniania posiadanych informacji w formie ustnej, papierowej bądź elektronicznej, stosownie do planów postępowania z ryzykiem; 3) administratorzy w zakresie odpowiedniego przechowywania kopii zapasowych, nośników (zawierających dane osobowe), odpowiedniej konfiguracji infrastruktury sieciowej, jej zabezpieczeń, jak również mechanizmów szyfrujących, 4) Za rozliczalność przetwarzanych danych odpowiedzialni są: a) administratorzy techniczni w zakresie odpowiedniej konfiguracji oraz weryfikacji zapisów dzienników systemowych, b) bezpośredni przełożony użytkownika w zakresie nadzoru nad czynnościami użytkownika w systemie. Za ochronę fizyczną przetwarzanych danych osobowych odpowiedzialny jest CIRF, do którego zadań należy tworzenie planu ochrony instytucji. Za nadzór nad zapewnieniem prawidłowego działania zabezpieczeń organizacyjnych w zakresie integralności, poufności, rozliczalności danych odpowiadają: kierujący poszczególnymi komórkami w zakresie właściwości w powiązaniu do powierzonych im zasobów.
Firmy zewnętrzne	Podmioty uprawnione spoza KAS, które uzyskały uprawnienia dostępowe do RNP.

4 ZAKRES DOKUMENTU

Niniejszy dokument określa zasady: ochrony informacji przetwarzanych w RNP, nadawania, modyfikacji i odbierania uprawnień w systemie, obszarów przetwarzania, zasobów technicznych RNP, oraz postępowania użytkowników RNP.
Dokument przeznaczony jest dla użytkowników i administratorów systemu RNP. Wykorzystywanie przedstawionych w dokumencie środków i metod zabezpieczenia systemu powinno odbywać się w warunkach zapewniających zachowanie wymaganego poziomu bezpieczeństwa przetwarzanych danych. Wszelkie zmiany w konfiguracji środowiska techniczno-systemowego lub w obszarach organizacyjno-prawnych wpływające na zmianę w podejściu do eksploatowanych środków ochrony systemu lub zmieniające bezpośrednio zastosowane środki ochrony będą uwzględniane w kolejnych wersjach IZSI RNP.

5 UDZIELANIE UPRAWNIEŃ DO PRZETWARZANIA DANYCH

Z uwagi na zróżnicowany charakter podmiotów uprawnionych / wierzycieli, zasady nadawania i zarządzania uprawnieniami w systemie podzielono na grupy podmiotów i dla każdej z grup opracowano odrębny formularz określający zakres niezbędnych danych w celu nadania uprawnień w systemie. Jednostka ubiegająca się o nadanie uprawnień powinna złożyć pisemny wniosek do Dyrektora Izby Administracji Skarbowej w Szczecinie uzupełniony o wypełniony formularz, właściwy dla jednostki wnioskującej. Opis i przeznaczenie poszczególnych formularzy dla nadawania i modyfikacji uprawnień znajdują się w pkt 4.2. Aktualne formularze RNP-1, RNP-2, RNP-3, RNP-4 oraz RNP-US, instrukcje i informacje dotyczące systemu RNP publikowane są na stronie BIP Izby Administracji Skarbowej w Szczecinie, pod adresem:
http://www.zachodniopomorskie.kas.gov.pl/izba-administracji-skarbowej-w-szczecinie/zalatwianie-spraw/rejestr-naleznosci-publicznoprawnych

5.1 ZAKRES UPRAWNIEŃ

Wykaz rodzajów uprawnień dostępowych w systemie RNP publikowany jest w aktualnej wersji na stronie BIP Izby Administracji Skarbowej w Szczecinie, pod adresem:
http://www.zachodniopomorskie.kas.gov.pl/izba-administracji-skarbowej-w-szczecinie/zalatwianie-spraw/rejestr-naleznosci-publicznoprawnych

5.2 FORMULARZE DO NADAWANIA UPRAWNIEŃ W RNP

- Każdy z formularzy przeznaczony jest dla odrębnej grupy podmiotów uprawnionych / wierzycieli. W celu właściwego doboru formularza należy zapoznać się z opisami umieszczonymi pod ich nazwami.
- W przypadku formularzy o następujących kodach: RNP-1, RNP-2, RNP-3 oraz RNP-4 w zakresie nadanie uprawnień dostępu do RNP żaden nie stanowi samodzielnego wniosku w rozumieniu § 2 ust. 1 ani też § 3 ust. 1 rozporządzenia Ministra Finansów z dnia 4 czerwca 2018 r. w sprawie Rejestru Należności Publicznoprawnych (Dz. U. z 2018 r. poz. 1124). Są one tylko załącznikami do wniosku o nadanie uprawnień do RNP (loginu i hasła), a ich rolą jest zaopatrzenie organu prowadzącego rejestr w niezbędne informacje o podmiocie wnioskującym oraz pracowniku, który otrzyma dostęp do rejestru.
- W przypadku formularzy o następujących kodach: RNP-1, RNP-2, RNP-3 w zakresie w jakim dotyczą one:
    a) zamknięcia konta dostępu do PUE,
    b) częściowego odebrania uprawnień,
    c) odblokowania konta PUE (bez zmiany hasła),

d) resetowania hasła,
e) aktualizacji danych dot. konta na PUE,
f) korekty formularza RNP,

każdy z formularzy stanowi samodzielny wniosek i składany jest bez dodatkowego pisma przewodniego.

- W przypadku formularza o kodzie RNP-US w zakresie:
  a) nadania uprawnień dostępu do RNP,
  b) zamknięcia konta dostępu do PUE,
  c) częściowego odebrania uprawnień,
  d) odblokowania konta PUE (bez zmiany hasła),
  e) resetowania hasła,
  f) aktualizacji danych dot. konta na PUE,
  g) korekty formularza RNP,

  stanowi on samodzielny wniosek i składany jest bez dodatkowego pisma przewodniego.
- Formularze RNP-1, RNP-2, RNP-3 oraz RNP-4 jeżeli dotyczą nadania uprawnień dostępu do RNP, sporządza się wyłącznie w postaci elektronicznej a następnie dołącza do właściwego wniosku o nadanie uprawnień opatrzonego kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP i jako załącznik przesyła wraz z wnioskiem na elektroniczną skrzynkę podawczą ePUAP Dyrektora Izby Administracji Skarbowej w Szczecinie.
- Formularze RNP-1, RNP-2, RNP-3 oraz RNP-4 (w przypadku: zamknięcia konta dostępu do PUE, częściowego odebrania uprawnień, odblokowania konta PUE, resetowania hasła, aktualizacji danych dot. konta na PUE, korekty formularza RNP) sporządza się wyłącznie w postaci elektronicznej i podpisuje kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP. Podpisane formularze przesyła się na elektroniczną skrzynkę podawczą ePUAP Dyrektora Izby Administracji Skarbowej w Szczecinie.
- Formularz RNP-US sporządza się w wersji papierowej. Po podpisaniu skan wniosku przesyła się na adres e-mail Izby Administracji Skarbowej w Szczecinie rnp-helpdesk.ias.szczecin@mf.gov.pl. Papierową wersję podpisanego wniosku należy przesłać przez operatora pocztowego na adres Izby Administracji Skarbowej w Szczecinie: ul. Roosevelta 1, 2, 70-525 Szczecin – z dopiskiem na kopercie „WNIOSEK RNP-US”.

RNP-1 Załącznik do wniosku jednostki samorządu terytorialnego o nadanie uprawnień dostępowych do danych w Rejestrze Należności Publicznoprawnych

Opis: formularz przeznaczony jest dla jednostek samorządu terytorialnego, które występują o uprawnienia jako wierzyciel lub podmiot uprawniony w RNP.

Zakres możliwych uprawnień:

- wprowadzanie / zmiana / wykreślanie danych z RNP,
- dostęp do danych w RNP,
- stosowanie ułatwionego sposobu wyszukiwania zobowiązanych w rejestrze obejmującego więcej niż jednego zobowiązanego.

RNP-2 Załącznik do wniosku jednostki administracji publicznej o nadanie uprawnień dostępowych do danych w Rejestrze Należności Publicznoprawnych

Opis: formularz przeznaczony jest dla następujących jednostek administracji publicznej:

1. Sądowy lub administracyjny organ egzekucyjny:
   a) Komornik sądowy
   b) Właściwy organ gminy o statusie miasta

c) Dyrektor oddziału Zakładu Ubezpieczeń Społecznych
d) Dyrektor oddziału regionalnego Agencji Mienia Wojskowego

2. Sąd
3. Organ prokuratury
4. Szef Centralnego Biura Antykorupcyjnego

- które występują o uprawnienia jako podmiot uprawniony w RNP.

Zakres możliwych uprawnień:

- dostęp do danych w RNP,
- stosowanie ułatwionego sposobu wyszukiwania zobowiązanych w rejestrze obejmującego więcej niż jednego zobowiązanego.

RNP-3 Załącznik do wniosku BIK-u / BIG-u o nadanie uprawnień dostępowych do danych w Rejestrze Należności Publicznoprawnych

Opis: formularz przeznaczony jest dla:

a) Biura Informacji Kredytowej,
b) biur informacji gospodarczej,

które występują o uprawnienia jako podmiot uprawniony w RNP.

Zakres możliwych uprawnień:

- dostęp do danych w RNP,
- stosowanie ułatwionego sposobu wyszukiwania zobowiązanych w rejestrze obejmującego więcej niż jednego zobowiązanego.

RNP-4 Oświadczenie podmiotu uprawnionego o spełnieniu wymagań dla ułatwionego sposobu wyszukiwania zobowiązanych w RNP

Opis: formularz przeznaczony jest dla:

a) urzędów skarbowych,
b) jednostek samorządu terytorialnego,
c) komorników sądowych,
d) organów gminy o statusie miasta,
e) Zakład Ubezpieczeń Społecznych,
f) oddziałów regionalnych Agencji Mienia Wojskowego,
g) sądów,
h) organów Prokuratury,
i) Centralnego Biuro Antykorupcyjnego,
j) Biura Informacji Kredytowej,
k) biur informacji gospodarczej,

- które jako podmiot uprawniony w RNP, na podstawie art. 18q § 2 ustawy z dnia 17 czerwca 1966r. o postępowaniu egzekucyjnym w administracji (Dz. U. z 2018 r., poz. 1314) zamierzają złożyć odrębny wniosek na ułatwiony sposób wyszukiwania zobowiązanych w rejestrze obejmujący więcej niż jednego zobowiązanego. Oświadczenie RNP-4 składane jest wraz z odpowiednim dla danego podmiotu formularzem: RNP-1, RNP-2, RNP-3 lub RNP-US.

RNP-US Wniosek urzędu skarbowego o nadanie / zmianę / odebranie uprawnień dostępowych do danych w Rejestrze Należności Publicznoprawnych.

Formularz przeznaczony jest dla urzędów skarbowych, które występują o nadanie, zmianę lub odebranie uprawnień jako podmiot uprawniony w RNP, a także o odblokowanie konta PUE i resetowanie hasła dostępu do konta portalowego PUE.

Zakres możliwych uprawnień:

- wprowadzanie / zmiana / wykreślanie danych z RNP,
- dostęp do danych w RNP,
- stosowanie ułatwionego sposobu wyszukiwania zobowiązanych w rejestrze obejmującego więcej niż jednego zobowiązanego.

5.3 KOMPETENCJE W ZARZĄDZANIU KONTAMI PORTALOWYMI PUE

W zależności od poziomu uprawnień dostępowych do RNP nadawane są one przez Organ RNP lub administratora lokalnego (ASI). W przypadku uprawnień dostępowych na poziomie administratora:

- RNP Wierzyciel Admin,
- RNP Uprawniony Admin,
- RNP Uprawniony Admin Wyszuk.Uł,
- RNP Uprawniony Ośw Admin,
- RNP Uprawniony Adm Ośw Wyszuk.Uł

są one nadawane wyłącznie przez Organ RNP.

Wszelkie pozostałe uprawnienia:

- RNP Wierzyciel,
- RNP Uprawniony,
- RNP Uprawniony Wyszukiwanie.Uł,
- RNP Uprawniony Ośw,
- RNP Uprawniony Ośw Wyszuk.Uł

są nadawane przez administratora lokalnego (który otrzymał stosowne uprawnienie na poziomie administratora) dla pracowników w jednostce (wierzyciela / podmiotu uprawnionego), w której świadczy pracę.

Szczegółowy wykaz kompetencji w zarządzaniu kontami portalowymi PUE dla RNP (wg rodzajów uprawnień) znajduje się na stronie BIP Izby Administracji Skarbowej w Szczecinie pod adresem: http://www.zachodniopomorskie.kas.gov.pl/izba-administracji-skarbowej-w-szczecinie/zalatwianie-spraw/rejestr-naleznosci-publicznoprawnych w pliku pt. Zarządzanie uprawnieniami RNP- kompetencje.pdf.

5.4 NADAWANIE UPRAWNIEŃ W RNP PRZEZ ADMINISTRATORÓW LOKALNYCH ASI

- Zasady oraz tryb nadawania kolejnych uprawnień dostępowych do danych z Rejestru Należności Publicznoprawnych dla pracowników danej jednostki organizacyjnej przez administratorów lokalnych ASI, odbywa się wg procedur ustalonych wewnątrz jednostki wierzyciela / podmiotu uprawnionego.
- Organ RNP nie odpowiada za zasady dystrybucji uprawnień dostępowych na poziomie:
    a) RNP Wierzyciel,

b) RNP Uprawniony,
c) RNP Uprawniony Wyszukiwanie.Uł,
d) RNP Uprawniony Ośw,
e) RNP Uprawniony Ośw Wyszuk.Uł

pozostawiając je do wyłącznej kompetencji wierzyciela / podmiotu uprawnionego.

- Należy pamiętać, iż użytkownik dla którego tworzony jest profil w PUE przez administratora lokalnego ASI musi posiadać upoważnienie do przetwarzania danych osobowych w zbiorach danych osobowych, wydane przez wierzyciela / podmiot uprawniony.

6 ROZPOCZYNANIE, ZAWIESZANIE I KOŃCZENIE PRACY W SYSTEMIE RNP

6.1 ZASADY ROZPOCZĘCIA PRACY

- Pracę w systemie rozpoczyna się od zainicjowania procesu identyfikacji i autoryzacji użytkownika. Użytkownik przechodzi poprzez proces logowania używając swojego identyfikatora oraz hasła.
- Uwierzytelnienie użytkownika odbywa się zgodnie z komunikatami zgłaszanymi przez system.
- Brak zadeklarowanego identyfikatora w bazie danych lub podanie przez użytkownika niewłaściwych danych powoduje odmowę dostępu do systemu.
- W przypadku pozytywnego przejścia procesu uwierzytelniania użytkownika o określonym identyfikatorze następuje proces autoryzacji.
- Autoryzacja w systemie polega na udostępnieniu użytkownikowi tylko tych zasobów, do których zostały mu nadane wcześniej uprawnienia (dotyczy to zarówno funkcjonalności jak i uprawnień dotyczących dostępu do danych składowanych w systemie).
- Rozpoczynając prace z systemem należy zwrócić szczególną uwagę na niestandardowe komunikaty wyświetlane przez system, a wszystkie anormalne zachowania systemu użytkownik powinien zgłosić do ASI.
- Identyfikacja i autoryzacja w RNP następuje z wykorzystaniem formularza logowania dostępnego na stronie https://pue.mf.gov.pl/eServices/_/

Uwaga: wyłączną przeglądarką internetową obsługującą RNP jest Mozilla Firefox. W przypadku logowania się do systemu RNP za pośrednictwem innych niż wskazana powyżej przeglądarek internetowych, istnieje ryzyko braku możliwości poprawnego uruchomienia serwisu.

6.2 ZASADY ZAWIESZANIA PRACY W SYSTEMIE

Podczas przerw w pracy z systemem, użytkownik ma obowiązek wylogowania się z systemu lub zablokowania stacji roboczej w celu uniemożliwienia osobom nieuprawnionym dostępu do danych systemu. Blokowanie dostępu do systemu operacyjnego następuje poprzez naciśnięcie przycisków Ctrl+Alt+Delete oraz kliknięcie w „Zablokuj ten komputer” (lub skrótem klawiaturowym: Logo Windows + L). Użytkownik systemu zobowiązany jest również stosować na swojej stacji roboczej wygaszacz ekranu chroniony hasłem.

6.3 ZASADY ZAKOŃCZENIA PRACY W SYSTEMIE

Przed zakończeniem pracy z systemem, użytkownik zobowiązany jest zapisać i zakończyć wszystkie aktywne procesy w aplikacji. Następnie należy zakończyć pracę z systemem poprzez bezpieczne wylogowanie z systemu oraz wyłączenie sprzętu komputerowego. Niedozwolone jest wyłączanie stacji roboczej przed zamknięciem aplikacji. Przed opuszczeniem pomieszczenia należy we właściwy sposób zabezpieczyć dokumenty oraz nośniki danych. Pomieszczenie powinno zostać zabezpieczone przed nieuprawnionym dostępem.

7 TWORZENIE KOPII ZAPASOWYCH I NOŚNIKÓW INFORMACJI

Informacja w systemie RNP przechowywana jest w centralnej bazie danych. Baza ta jest objęta polityką utrzymania kopii bezpieczeństwa za pomocą mechanizmów bazy danych (kopie na taśmę) oraz migawkami na poziomie macierzy dyskowej, pozwalającymi na szybkie odzyskanie danych. Baza danych jest skonfigurowana w trybie archivelog, który pozwala na odzyskanie informacji do chwili wystąpienia awarii. Dodatkowo centralna baza danych posiada niezależną kopię synchronizowaną na bieżąco i utrzymywaną w ośrodku zapasowym.

8 ZABEZPIECZENIA SYSTEMU PRZETWARZAJĄCEGO DANE OSOBOWE

8.1 ŚRODKI FIZYCZNE

Dla zapewnienia odpowiedniego bezpieczeństwa fizycznego w systemie RNP stosuje się środki ochrony fizycznej dotyczące odpowiedniego zabezpieczenia serwera bazodanowego, sprzętu sieciowego (urządzeń aktywnych), okablowania, nośników informacji, systemów zasilania i klimatyzacji, zgodnie z obowiązującymi w tym zakresie standardami i wytycznymi.
Pozostałe komponenty związane z RNP: sprzęt informatyczny użytkowników oraz dokumenty papierowe zawierające dane osobowe podlegają ochronie fizycznej określonej w politykach ochrony danych osobowych poszczególnych jednostek organizacyjnych.
Dla serwerowni, w której znajduje się infrastruktura związana z systemem RNP zastosowano następujące środki:

Środki ochrony fizycznej danych		
W tej grupie środków należy zaznaczyć pozycje, które odnoszą się do fizycznego zabezpieczenia przetwarzanych danych osobowych		
1	-	Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi).
2	X	Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności ogniowej >= 30 min.
3	-	Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności na włamanie - drzwi klasy C.
4	X	Zbiór danych osobowych przechowywany jest w pomieszczeniu, w którym okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej.
5	X	Pomieszczenie, w którym przetwarzany jest zbiór danych osobowych wyposażone jest w system alarmowy przeciwwłamaniowy.
6	X	Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych objęty jest systemem kontroli dostępu.
7	X	Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych.
8	X	Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych podczas nieobecności pracowników jest nadzorowany przez służbę ochrony.
9	-	Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych przez całą dobę jest nadzorowany przez służbę ochrony.
10	-	Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej szafie niemetalowej.
11	-	Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej szafie metalowej.
12	-	Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętym sejfie lub kasie pancernej.
13	-	Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej szafie niemetalowej.
14	-	Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej szafie metalowej.

15	-	Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętym sejfie lub kasie pancernej.
16	-	Zbiory danych osobowych przetwarzane są w kancelarii tajnej, prowadzonej zgodnie z wymogami określonymi w odrębnych przepisach.
17	X	Pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy.
18	-	Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

8.2 ŚRODKI TECHNICZNE

W systemie RNP zastosowano następujące techniczne środki ochrony:

- macierze dyskowe oraz mechanizmy replikacji danych,
- system tworzenia kopii zapasowych wraz z procedurami zarządzania nośnikami do wykonywania i odtwarzania kopii zapasowych,
- stosowane są systemy podtrzymywania napięcia,
- redundancja,
- system chroniony jest przed szkodliwym oprogramowaniem za pomocą systemu antywirusowego,
- liczba kont administratorów jest ograniczona,
- dostęp do systemu jest realizowany wyłącznie przez autoryzowanych użytkowników,
- stosowane są mechanizmy ochrony kryptograficznej z wykorzystaniem certyfikatów i kluczy kryptograficznych,
- przez serwer bazy danych zapewnione są mechanizmy integralności danych na poziomie struktury danych,
- użytkownicy posiadają minimalny poziom uprawnień zapewniający realizację zadań służbowych,
- stosuje się mechanizmy kontroli dostępu do danych. Użytkownicy logują się do systemu podając swój identyfikator i hasło. Konto użytkownika przypisane i wykorzystywane jest tylko przez jednego, uprawnionego użytkownika systemu.
- w celu zabezpieczenia danych przed utratą, wykonywane są kopie zapasowe danych systemu. Do backupu dostęp mają tylko upoważnieni pracownicy.
- na stacjach roboczych użytkowników systemu stosuje się ochronę antywirusową oraz system filtracji stron www,
- minimalna długość haseł wynosi min. 8 znaków zawierających małe i wielkie litery oraz cyfry lub znaki specjalne. Zmiana hasła dokonywana jest maksymalnie co 30 dni.

8.3 ŚRODKI ORGANIZACYJNE

Zapewnienie odpowiedniego bezpieczeństwa organizacyjnego w systemie RNP osiągnięto poprzez określenie właściciela systemu, właściwego podziału zadań i ról w systemie, wyznaczenie administratorów systemu, określenie poziomów dostępu dla użytkowników systemu wynikających z wewnętrznych procedur oraz regulacji, określenie odpowiedzialności administratorów i użytkowników systemu. Zastosowano politykę kont imiennych wraz z kontrolą uprawnień. Opisane zostały role i przypisano do nich zakresy przetwarzanych informacji. Dane uwierzytelniające do silnych kont technicznych powierzone i przechowywane są w warunkach zapewniających brak możliwości ich ujawnienia przez administratorów infrastruktury (CIRF).

9 NARUSZENIE BEZPIECZEŃSTWA INFORMACJI W SYSTEMIE

W systemie RNP zastosowano mechanizmy związane z zarządzaniem bezpieczeństwa danych osobowych w systemie, chroniące system przed naruszeniem bezpieczeństwa danych osobowych, w tym będące przyczyną: naruszenia zasobów, utraty poufności, integralności, rozliczalności, dostępności informacji lub zmniejszenia niezawodności systemu. Za naruszenie bezpieczeństwa danych osobowych przetwarzanych za pomocą systemu informatycznego RNP uważa się każde określone zdarzenie lub działanie łamiące zasady ochrony informacji, w szczególności takie, które może powodować utratę poufności, integralności lub ograniczenia dostępności do danych osobowych. Z każdego zdarzenia naruszającego bezpieczeństwo informacji osoba, która zauważyła zdarzenie sporządza notatkę służbową w sprawie dla LADO lub do IOD.

9.1 ZGŁASZANIE ZDARZEŃ ZWIĄZANYCH Z NARUSZENIEM BEZPIECZEŃSTWA

Zaobserwowane przypadki naruszenia bezpieczeństwa informacji w systemie RNP lub podejrzenia wystąpienia takiego naruszenia przez użytkownika systemu należy zgłaszać IOD lub bezpośrednio do LADO systemu RNP. W przypadku potwierdzenia zaistnienia incydentu bezpieczeństwa IOD lub LADO przekazują informacje do ADO oraz do ASI w celu uruchomienia procedury zarządzania incydentami.

9.2 ZARZĄDZANIE INCYDENTAMI ZWIĄZANYMI Z BEZPIECZEŃSTWEM INFORMACJI

W przypadku zaobserwowania lub podejrzenia przez użytkownika wystąpienia naruszenia bezpieczeństwa informacji w systemie RNP należy:

- bez zbędnej zwłoki zgłosić taki przypadek IOD lub bezpośrednio LADO systemu RNP,
- w miarę możliwości zabezpieczyć dowody naruszenia bezpieczeństwa informacji.

IOD lub LADO przyjmuje zgłoszenie oraz niezwłocznie podejmuje (w porozumieniu z ASI) działania mające na celu ograniczenie zasięgu incydentu oraz zapobieżenie ewentualnego jego wykorzystania. Następnie podejmowane są działania korygujące mające na celu wyeliminowanie zauważonej słabości systemu zabezpieczeń, zgodnie z obowiązującymi w IAS Szczecin procedurami.

10 ZABEZPIECZENIA KRYPTOGRAFICZNE

Transmisja danych między stacją końcową systemu a serwerami centralnymi podlega mechanizmom szyfrowania i zapewnienia integralności w oparciu o SSL.

11 PRZEGLĄDY, KONSERWACJE I NAPRAWY

Dla systemu przewiduje się rutynowe wykonywanie przeglądów pod kątem niezawodności, wydajności oraz instalowania poprawek rekomendowanych przez dostawców wykorzystywanego oprogramowania. Ponadto przewiduje się rutynowe wykonywanie testów niezawodności oraz możliwości przywracania danych po awarii.