POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

W SYSTEMIE

REJESTR NALEŻNOŚCI PUBLICZNOPRAWNYCH

Nazwa	**POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH W SYSTEMIE 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	14.06.2019	Podpis	A. Żurawski
Akceptacja w zakresie zabezpieczeń technicznych **Dział Bezpieczeństwa i Ochrony Informacji (IWO)**	Imię i nazwisko, stanowisko	Eugeniusz Pietrzak Kierownik	Data	17.06.2019	Podpis	Kierownik Działu Eugeniusz Pietrzak
Akceptacja w zakresie zabezpieczeń technicznych **Pion Informatyki (IZPI)**	Imię i nazwisko, stanowisko	Damian Garczyński z-ca DIAS	Data	17.06.2019	Podpis	Z-ca Dyrektora Izby Administracji Skarbowej w Szczecinie Damian Garczyński
Akceptacja w zakresie merytorycznym (biznesowym) **Pion Poboru i Egzekucji (IZPE)**	Imię i nazwisko, stanowisko	Anita Sikorska z-ca DIAS	Data	17.06.2019 r.	Podpis	Z-ca Dyrektora Izby Administracji Skarbowej w Szczecinie Anita Sikorska
Zatwierdził	Imię i nazwisko, stanowisko	DIAS	Data	17/06/19	Podpis	Dyrektor Izby Administracji Skarbowej w Szczecinie Jarosław Grzelak

SPIS TREŚCI

1 WYKAZ SKRÓTÓW I TERMINÓW

1)	**AD**	Active Directory
2)	**ADO**	Administrator Danych Osobowych – Dyrektor Izby Administracji Skarbowej w Szczecinie
3)	**ASI**	Administrator Systemu Informatycznego
4)	**CIRF**	Centrum Informatyczne Resortu Finansów
5)	**CRP-KEP**	Centralny Rejestr Podmiotów - Krajowa Ewidencja Podatników
6)	**DIAS**	Dyrektorzy Izb Administracji Skarbowej
7)	**IAS**	Izba Administracji Skarbowej
8)	**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.
9)	**Instrukcja**	Instrukcja nadawania loginu i hasła do RNP przez administratora lokalnego
10)	**IOD**	Inspektor Ochrony Danych
11)	**IZSI RNP**	Instrukcja Zarządzania Systemem Informatycznym RNP
12)	**Jednostka organizacyjna**	komórki organizacyjne, izby administracji skarbowej, urzędy skarbowe
13)	**JST**	Jednostki samorządu terytorialnego
14)	**KAS**	Krajowa Administracja Skarbowa
15)	**KRI**	Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247)
16)	**LADO**	Lokalny Administrator Danych Osobowych
17)	**MF**	Ministerstwo Finansów
18)	**Minister**	Minister właściwy do spraw budżetu, finansów publicznych i instytucji finansowych obsługiwany przez Ministerstwo Finansów
19)	**NUS**	Naczelnicy Urzędów Skarbowych
20)	**Organ RNP**	Organ prowadzący rejestr (RNP) - Dyrektor Izby Administracji Skarbowej w Szczecinie
21)	**PBDO RNP**	Polityka Bezpieczeństwa Danych Osobowych w Systemie RNP
22)	**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.)
23)	**pracownik**	Funkcjonariusz, pracownik, stażysta, praktykant, wolontariusz, pracownik zleceniowy.
24)	**RNP**	Rejestr Należności Publicznoprawnych
25)	**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)
26)	**SSP**	Komponent systemu e-Podatki realizujący m.in. zbiór funkcjonalności RNP
27)	**Szef KAS**	Szef Krajowej Administracji Skarbowej
28)	**uodo**	Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r., poz. 1000)

29)	**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.)
30)	**US**	Urząd skarbowy
31)	**Użytkownik**	pracownik przetwarzający dane w RNP zatrudniony przez ADO, wierzyciela lub podmiot uprawniony
32)	**Wierzyciel**	Jednostka samorządu terytorialnego lub naczelnik urzędu skarbowego
33)	**Zainteresowany**	Podmiot, któremu udostępnia się dane z systemu RNP
34)	**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 dokumentu jest przedstawienie zagadnień związanych z bezpieczeństwem przetwarzania danych osobowych w systemie RNP.

Przedstawiono w nim obowiązujące uregulowania organizacyjno-prawne mające wpływ na bezpieczeństwo danych w RNP i odnoszące się do wdrożonych środków ochrony.

Niniejszy dokument dotyczy danych osobowych przetwarzanych na mocy przepisów prawa Unii Europejskiej oraz prawa krajowego, zarówno w sposób tradycyjny, jak i elektroniczny.

Zasady określone w niniejszym opracowaniu obowiązują wszystkich użytkowników.

Dokument zawiera ogólny opis RNP oraz zidentyfikowanych i zastosowanych mechanizmów zapewniających bezpieczeństwo przetwarzanych w nim danych osobowych.

3 ODPOWIEDZIALNOŚĆ

Dokument jest dedykowany wszystkim osobom i podmiotom odpowiedzialnym za prawidłowe funkcjonowanie Rejestru Należności Publicznoprawnych oraz za jego eksploatację (DIAS, NUS, CIRF, 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, obszarów przetwarzania, zasobów technicznych RNP, oraz zasady postępowania użytkowników RNP.

Dokument opisuje infrastrukturę sprzętowo-systemową Rejestru Należności Publicznoprawnych oraz umiejscowienie Rejestru w ramach eksploatowanych systemów informatycznych. Dokument zawiera opis wzajemnych relacji wewnątrz systemu oraz powiązań z systemami informatycznymi bezpośrednio związanymi z Rejestrem. Informacje zawarte w niniejszym dokumencie są zgodne ze stanem faktycznym środowiska RNP na 06.06.2019 r. 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 PBDO RNP.

5 POWIĄZANIA Z INNYMI DOKUMENTAMI

5.1 AKTY NORMATYWNE

- Ustawa z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej (Dz. U. z 2019 r., poz. 768 z późn. zm.).
- Ustawa z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz. U. z 2018 r., poz. 1314 z późn. zm.).
- Ustawa z dnia 13 października 1995 r. o zasadach ewidencji i identyfikacji podatników i płatników (Dz. U. 2019 r., poz.63 z późn. zm.).
- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r., poz. 1000).
- Ustawa z dnia 7 kwietnia 2017 r. o zmianie niektórych ustaw w celu ułatwienia dochodzenia wierzytelności (Dz. U. z 2017 r., poz. 933 z późn. zm.).
- Ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2018 r., poz. 2096 z późn. zm.).
- Ustawa z dnia 29 sierpnia 1997 r. Ordynacja podatkowa (Dz. U. 2018 r., poz. 800 z późn. zm.).
- Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2019 r., poz. 700).
- Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz.U. 2018 r., poz.2187).
- Ustawa z dnia 9 kwietnia 2010 r. o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych (Dz. U. z 2019 r. poz. 681, z późn. zm.).
- Ustawa z dnia 13 listopada 2003 r. o dochodach jednostek samorządu terytorialnego (Dz. U. 2018 r., poz. 1530 z późn. zm.).
- Rozporządzenie Ministra Finansów z dnia 4 czerwca 2018 r. w sprawie Rejestru Należności Publicznoprawnych (Dz. U. z 2018. poz. 1124).

- Rozporządzenie 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)
- Zarządzenie Ministra Rozwoju i Finansów z dnia 1 marca 2017 r. w sprawie organizacji jednostek organizacyjnych Krajowej Administracji Skarbowej oraz nadania im statutów (Dz. Urz. MRiF poz. 41).

5.2 REGULACJE WEWNĘTRZNE

Dokumentacje (m. in. polityki, procedury, instrukcje) dotyczące przetwarzania danych osobowych wszystkich podmiotów uprawnionych, którym udostępniane są dane z RNP.

5.3 NORMY I STANDARDY

Na kontekst przetwarzania danych osobowych składają się niżej wymienione przepisy:

- 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 - RODO).
- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018, poz. 1000 z późn. zm.).
- Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247).
- Zarządzenie Ministra Rozwoju i Finansów z dnia 28 lutego 2017 r. w sprawie wprowadzenia instrukcji kancelaryjnej izb administracji skarbowej, urzędów skarbowych i urzędów celno-skarbowych oraz instrukcji w sprawie organizacji i zakresu działania archiwum zakładowego izb administracji skarbowej (Dz. Urz. MRiF poz. 43).

Normy:

- PN ISO/IEC 27000:2017-06 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji . Przegląd i terminologia.
- PN ISO/IEC 27001:2017-06 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania.
- PN-ISO/IEC 27002:2017-06 Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji.
- PN ISO/IEC 27005:2014-01 Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji.

6 DEFINICJA SYSTEMU

6.1 NAZWA SYSTEMU

Rejestr Należności Publicznoprawnych – RNP

6.2 CEL PRZETWARZANIA DANYCH W SYSTEMIE

Rejestr Należności Publicznoprawnych jest rejestrem publicznym, przetwarzającym dane podmiotów, które pomimo obowiązku nie wykonują zapłaty należności pieniężnych podlegających egzekucji administracyjnej, dla których wierzycielami są naczelnicy urzędów skarbowych albo jednostki samorządu terytorialnego.

Celem istnienia RNP jest ułatwienie badania wiarygodności kontrahentów w obrocie gospodarczym, w taki sposób aby informacja o istotnych zaległościach była dostępna on-line, od ręki, zagregowana w jednym źródle.

6.3 KATEGORIE OSÓB, KTÓRYCH DANE DOTYCZĄ

Kategorie osób, których dane są przetwarzane w RNP określono w art. 18b § 2 u.p.e.a:

- osoby fizyczne,
- osoba fizyczna prowadząca działalność gospodarczą,
- osoba prawna lub jednostka organizacyjna niebędąca osobą prawną,
- nierezydent w rozumieniu przepisów Prawa dewizowego będący osobą fizyczną,
- nierezydent w rozumieniu przepisów Prawa dewizowego będący osobą fizyczną prowadzącą działalność gospodarczą,
- nierezydent w rozumieniu przepisów Prawa dewizowego będący osobą prawną lub jednostką organizacyjną niebędącą osobą prawną.

6.4 SPOSÓB ZBIERANIA DANYCH

W myśl art. 18b § 1 u.p.e.a. w rejestrze gromadzi się informacje o należnościach pieniężnych, podlegających egzekucji administracyjnej, dla których wierzycielem jest naczelnik urzędu skarbowego albo jednostka samorządu terytorialnego, jeżeli należności te wynikają:

1) z dokumentu, o którym mowa w art. 3 a § 1;
2) z decyzji, postanowienia lub innego orzeczenia, które jest ostateczne;
3) z prawomocnego wyroku, postanowienia lub mandatu karnego wydanego na podstawie przepisów Kodeksu karnego skarbowego lub Kodeksu karnego;
4) z mandatu karnego wydanego w postępowaniu w sprawach o wykroczenia;
5) bezpośrednio z przepisu prawa.

Zgodnie z art. 18 d § 5 u.p.e.a. wierzyciel wprowadza do rejestru, zmienia w rejestrze lub wykreśla z rejestru dane, za pośrednictwem funkcjonalności systemu teleinformatycznego, w którym prowadzony jest rejestr, udostępnianej na stronie podmiotowej urzędu obsługującego organ prowadzący rejestr.

7 OPIS SYSTEMU

7.1 LOKALIZACJA SYSTEMU

Miejsce przetwarzania danych gromadzonych w systemie RNP:

- Zlokalizowane w ośrodku przetwarzania danych CIRF w Radomiu serwery centralnej bazy danych,
- Umieszczone w pomieszczeniach CIRF stacje administracyjne przy pomocy których administratorzy techniczni wykonują swoje obowiązki służbowe,
- Pomieszczenia w których dane przetwarzają użytkownicy RNP zlokalizowane w budynkach: MF, IAS, US, oraz JST,
- Każde miejsce z którego zainteresowany, zobowiązany lub podmiot uprawniony, po uwierzytelnieniu, ma możliwość uzyskania odpowiednich informacji z RNP.

7.2 STRUKTURA ZBIORU DANYCH OSOBOWYCH

Zakres danych osobowych przetwarzanych w systemie RNP został określony art. 18b § 2 u.p.e.a i zawiera dane:

- osób fizycznych, obejmujące:

– imię i nazwisko,
– numer Powszechnego Elektronicznego Systemu Ewidencji Ludności (PESEL), jeżeli został nadany,
– datę urodzenia, jeżeli nie został nadany numer PESEL,

- osób fizycznych prowadzących działalność gospodarczą, obejmujące:

– imię i nazwisko,
– firmę,
– numer PESEL, jeżeli został nadany, numer identyfikacji podatkowej (NIP) lub numer identyfikacji w Krajowym Rejestrze Urzędowym Podmiotów Gospodarki Narodowej (REGON),

- osób prawnych lub jednostek organizacyjnych niebędących osobą prawną, obejmujące:

– firmę lub nazwę,
– NIP lub numer REGON,

- nierezydentów w rozumieniu przepisów Prawa dewizowego będących osobą fizyczną, obejmujące:

– imię i nazwisko,
– NIP albo kraj wydania i numer paszportu lub numer identyfikacyjny nadany w innym kraju, w szczególności numer podatkowy lub numer ubezpieczeniowy, jeżeli nierezydent nie posiada identyfikatora podatkowego,
– datę urodzenia, jeżeli nierezydent nie posiada NIP, paszportu lub numeru identyfikacyjnego nadanego w innym kraju,

- nierezydentów w rozumieniu przepisów Prawa dewizowego będących osobą fizyczną prowadzącą działalność gospodarczą, obejmujące:

– imię i nazwisko, firmę lub nazwę,
– NIP albo kraj wydania i numer paszportu lub numer identyfikacyjny nadany w innym kraju, w szczególności numer podatkowy lub numer ubezpieczeniowy, jeżeli nierezydent nie posiada numeru identyfikatora podatkowego,
– datę urodzenia albo adres miejsca prowadzenia działalności gospodarczej, w tym adres głównego miejsca prowadzenia działalności gospodarczej, jeżeli nierezydent nie posiada NIP, paszportu lub numeru identyfikacyjnego nadanego w innym kraju,

- nierezydentów w rozumieniu przepisów Prawa dewizowego będących osobą prawną lub jednostką organizacyjną niebędącą osobą prawną, obejmujące:

– firmę lub nazwę,
– NIP albo numer identyfikacyjny nadany w innym kraju, w szczególności numer podatkowy, jeżeli nierezydent nie posiada numeru identyfikatora podatkowego,
– adres siedziby, jeżeli nierezydent nie posiada NIP lub numeru identyfikacyjnego nadanego w innym kraju;

- oznaczenia wierzyciela;
- wysokości należności pieniężnej i odsetek z tytułu niezapłacenia jej w terminie, jeżeli pobiera się odsetki, wraz z rodzajem i podstawą prawną tej należności;
- informacji określonych w art. 18f § 1 i 2.

7.3 ODBIORCY DANYCH OSOBOWYCH

Dane z rejestru (o których mowa w art. 18b § 2 u.p.e.a) udostępniane są zobowiązanemu lub podmiotowi zainteresowanemu, po jego uwierzytelnieniu na portalu podatkowym przy użyciu danych weryfikowanych za pomocą kwalifikowanego certyfikatu podpisu elektronicznego albo profilu zaufanego ePUAP.

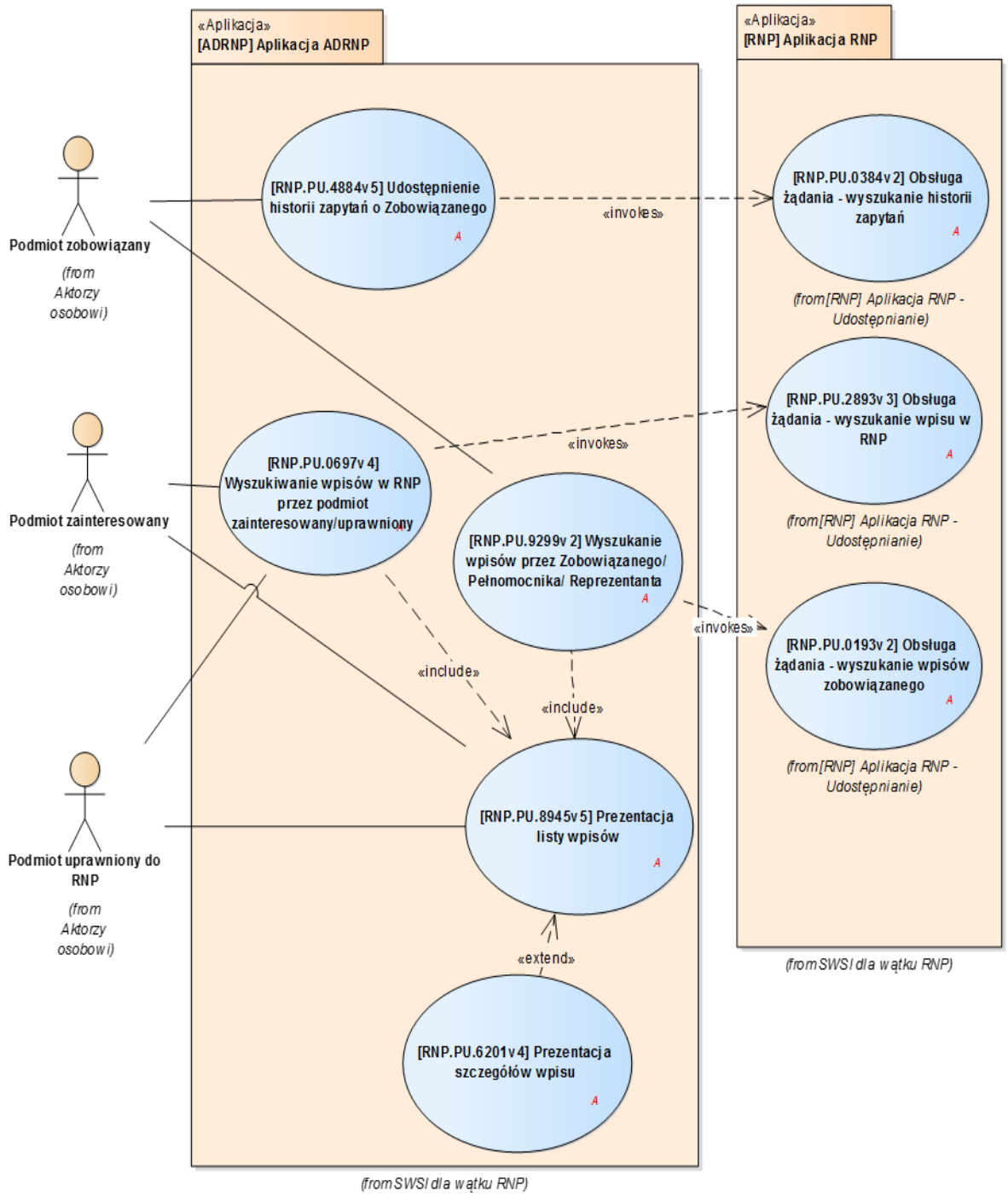
Kolejna grupa podmiotów posiadająca dostęp do rejestru to wierzyciele. Wierzyciel po uwierzytelnieniu w systemie, na podstawie podanego identyfikatora i hasła wprowadza do systemu teleinformatycznego, w którym prowadzony jest rejestr, dane, o których mowa w art. 18b § 2 u.p.e.a.

Za pośrednictwem funkcjonalności systemu teleinformatycznego udostępnionej na stronie podmiotowej urzędu obsługującego organ prowadzący rejestr, dane z tego rejestru udostępniane są również podmiotom uprawnionym, o których mowa w art. 18q § 2 u.p.e.a.:

1) wierzyciel,
2) sądowy lub administracyjny organ egzekucyjny,
3) sąd,

4) organ prokuratury,
5) Szef Centralnego Biura Antykorupcyjnego,
6) instytucje utworzone na podstawie art. 105 ust. 4 ustawy z dnia 29 sierpnia 1997 r. - Prawo bankowe,
7) biura informacji gospodarczej działające na podstawie ustawy z dnia 9 kwietnia 2010 r. o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych (Dz. U. z 2018 r. poz. 470, z późn. zm.).

Ponadto, dostęp do danych zawartych w rejestrze zapewnia się także osobom upoważnionym przez wierzycieli oraz organ prowadzący rejestr w zakresie, w jakim jest to niezbędne do nadzoru, konserwacji i rozwijania systemów informatycznych wierzycieli i systemu teleinformatycznego, w ramach którego prowadzony jest rejestr (art. 18r. u.p.e.a.).



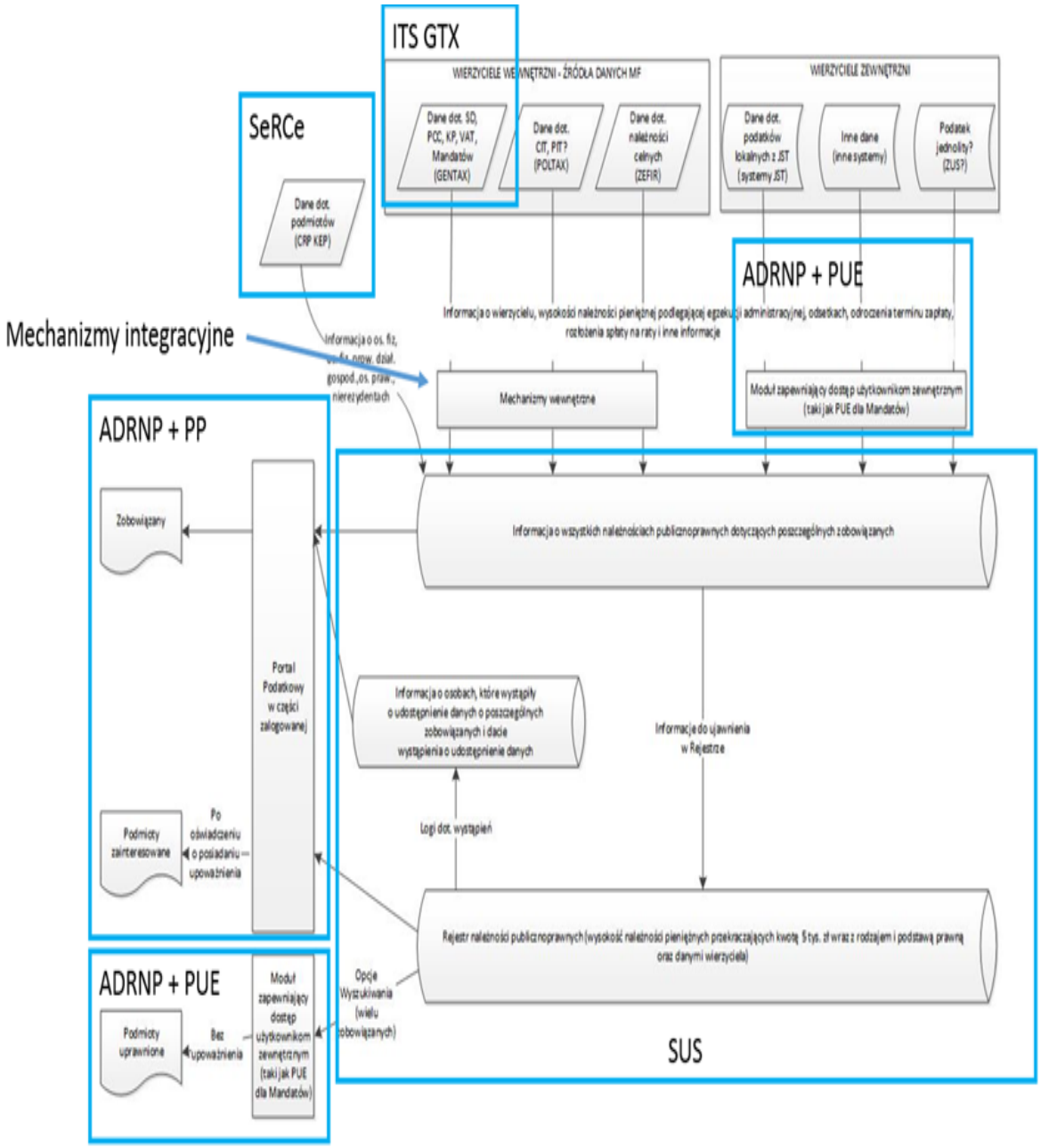
7.4 WYKAZ ZBIORÓW DANYCH OSOBOWYCH PRZETWARZANYCH ZA POMOCĄ SYSTEMU

W systemie RNP przetwarzane są dane określone w art. 18b §1 i 2 u.p.e.a.

7.5 SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI

RNP gromadzi i przetwarza dane, które są / mogą być pobierane z: CRP KEP, GENTAX, POLTAX, ZEFIR2, baz danych JST oraz podmiotów uprawnionych.

Obsługę aktualizacji danych jak i udostępnianie informacji z RNP dostarcza system ePodatki poprzez implementacje odpowiednich interaktywnych aplikacji udostępnianych w Internecie oraz interfejsów dla systemów wierzycieli.



8 BEZPIECZEŃSTWO FIZYCZNE, TECHNICZNE I ORGANIZACYJNE

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.

8.2 ŚRODKI TECHNICZNE

Opis zastosowanych środków przestawiono w IZSI RNP.

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. Wykaz zastosowanych środków organizacyjnych opisano w IZSI RNP.

9 NARUSZENIE ZASAD OCHRONY

Ryzyko naruszenia zasad ochrony danych osobowych w rozumieniu RODO jest redukowane poprzez zapobieganie zniszczeniu/utracie danych za pomocą środków technicznych (kopie bezpieczeństwa, uaktualniana na bieżąco baza w ośrodku zapasowym) oraz procesowych (testowanie zmian w celu wyeliminowania ew. błędów mogących doprowadzić do materializacji ewentualnych ryzyk).

Ryzyko przypadkowego lub niezgodnego z prawem zmodyfikowania danych redukowane jest poprzez umożliwienie wykonywania zmian wyłącznie przez uprawnioną aplikację, która podlega procesowi testowania pod kątem prawidłowości wykonywanego przetwarzania. Dodatkowo, użytkownicy mogący wykonywać zmiany podlegają procesowi zarządzania uprawnieniami i zakresem informacji, na którym mogą wykonywać zmiany (uprawnienia do konkretnego użytkownika) i rozliczalności wykonywanych operacji.

Ryzyka nieuprawnionego ujawnienia lub dostępu do danych osobowych jest redukowane poprzez proces zarządzania uprawnieniami dostępu, uwierzytelnianiem użytkowników końcowych oraz szyfrowanie transmisji sieciowej.

W przypadku wystąpienia naruszenia zasad ochrony, zastosowanie mają procedury obsługi incydentów w MF oraz lokalne procedury przyjęte u poszczególnych użytkowników zgodnie z lokalnymi politykami.

10 UPOWAŻNIENIA I SZKOLENIA

Użytkownicy mający dostęp do systemu RNP powinny: posiadać przeszkolenie z zakresu ochrony danych osobowych, mieć nadane upoważnienie do przetwarzania danych osobowych, być osobami uprawnionymi, dopuszczonymi przez administratora. Osoby upoważnione do przetwarzania danych osobowych, są zobligowane do pisemnego zobowiązania do zachowania poufności przetwarzania danych osobowych. Obowiązek ten nie wygasa w związku z ustaniem zatrudnienia.

W przypadku pracowników zatrudnionych w jednostkach niebędących organem KAS, którzy uzyskali stosowne uprawnienia dostępowe do RNP, odpowiedzialność w sprawie ww. wymagań (posiadanych upoważnień i szkoleń) ponoszą pracodawcy tych osób.