Obowiązuje od 16 maja 2024 roku

Polityka świadczenia usługi i deklaracja praktyk dla usługi rejestrowanego doręczenia elektronicznego w Poczcie Polskiej S.A.

wersja 3.1

Metryka dokumentu

Nazwa:	Polityka świadczenia usługi i deklaracja praktyk dla usługi rejestrowanego doręczenia elektronicznego w Poczcie Polskiej S.A.		
Identyfikator dokumentu	18/2024		
Wersja:	3.1	**Autor:**	Poczta Polska S.A.
Stron:	28	**Data:**	8.05.2024

1. Wstęp

1.1. Wprowadzenie

Niniejsza Polityka świadczenia usługi i deklaracja praktyk dla usługi rejestrowanego doręczenia elektronicznego w Poczcie Polskiej S.A. („**Polityka**”) określa ogólne zasady stosowane przez Pocztę Polską S.A. w trakcie świadczenia kwalifikowanej usługi rejestrowanego doręczenia elektronicznego. Polityka definiuje Strony Usługi RDE, określa ich obowiązki i odpowiedzialność oraz obszary zastosowań jej regulacji. Ponadto określa rozwiązania, w tym techniczne i organizacyjne, wskazujące warunki zabezpieczeń dla Usługi RDE.

1.2. Słownik

1. **Dane identyfikujące osobę** – zestaw danych umożliwiających ustalenie tożsamości osoby fizycznej lub prawnej, lub osoby fizycznej reprezentującej osobę prawną;
2. **Dostawca usług zaufania** – dostawca usługi zaufania (np. kwalifikowanej usługi elektronicznego znacznika czasu lub usługi zaawansowanej pieczęci elektronicznej), będący osobą fizyczną lub prawną, która świadczy przynajmniej jedną usługę zaufania, jako kwalifikowany dostawca usług zaufania;
3. **Z-ca Dyrektora CTC ds. Cyfryzacji** – Zastępca Dyrektora Centrum Transformacji Cyfrowej ds. Cyfryzacji w Poczcie Polskiej S.A.;
4. **ETSI** – normy Europejskiego Instytutu Norm Telekomunikacyjnych:
    1. ETSI EN 319 401 v2.2.1 *Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers,*
    2. ETSI EN 319 521 V1.1.1 *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers;*
5. **HSM** (ang. Hardware Security Module) – sprzętowy moduł bezpieczeństwa, stanowiący w pełni zabezpieczone urządzenie do przechowywania i zarządzania kluczami bezpieczeństwa do krytycznej autoryzacji i przetwarzania kryptograficznego oraz zapewniający całe spektrum zastosowań: od szyfrowania danych cyfrowych w procesach i transakcjach biznesowych, poprzez zabezpieczenie dokumentów elektronicznych w urzędach i instytucjach, po zarządzanie kluczami dostępu i bezpieczeństwo w ramach wymiany danych;
6. **Krajowy Schemat Identyfikacji** – krajowy schemat identyfikacji elektronicznej obejmujący:
    1) węzeł krajowy identyfikacji elektronicznej („węzeł krajowy”),
    2) przyłączone do węzła krajowego:
        a) systemy identyfikacji elektronicznej, w których wydawane są środki identyfikacji elektronicznej,
        b) systemy teleinformatyczne, w których udostępniane są usługi online,

3) węzeł wykorzystywany w procesie transgranicznego uwierzytelniania osób, o którym mowa w przepisach wydanych na podstawie Rozporządzenia eIDAS („węzeł transgraniczny”);

7. **Kwalifikowana Usługa RDE (Usługa RDE)** – kwalifikowana usługa rejestrowanego doręczenia elektronicznego, umożliwiająca przesłanie danych między stronami trzecimi drogą elektroniczną i zapewniająca dowody związane z posługiwaniem się przesyłanymi danymi, w tym dowód wysłania i otrzymania danych, oraz chroniąca przesyłane dane przed ryzykiem utraty, kradzieży, uszkodzenia lub jakiejkolwiek nieupoważnionej zmiany, spełniająca wymogi, o których mowa w art. 44 Rozporządzenia eIDAS;
8. **Kwalifikowany dostawca usług zaufania** – dostawca usług zaufania, któremu status kwalifikowany nadaje organ nadzoru;
9. **Personel** – osoby zatrudnione odpowiednio, przez Pocztę Polską S.A. lub Pocztę Polską Usługi Cyfrowe Sp. z o.o. na podstawie umowy o pracę oraz osoby fizyczne świadczące osobiście usługi na rzecz Poczty Polskiej S.A. lub Poczty Polskiej Usługi Cyfrowe Sp. z o.o. w oparciu o umowę cywilnoprawną (umowę o dzieło, umowę zlecenia, umowę o świadczenie usług), w tym członkowie zarządu i rady nadzorczej Poczty Polskiej S.A. lub Poczty Polskiej Usługi Cyfrowe Sp. z o.o.;
10. **Poziom wiarygodności (bezpieczeństwa)** – poziom bezpieczeństwa identyfikacji elektronicznej zgodnie z art. 8 Rozporządzenia eIDAS, określany niekiedy jako poziom zaufania lub wiarygodności (tłum. z j. ang. *Level of assurance);*
11. **Poczta Polska** – Poczta Polska S.A.;
12. **PPUC** – Poczta Polska Usługi Cyfrowe Sp. z o.o.;
13. **Przesyłka** – dane przesyłane pomiędzy stronami z wykorzystaniem usługi RDE;
14. **Regulamin** – Regulamin świadczenia kwalifikowanej usługi rejestrowanego doręczenia elektronicznego w Poczcie Polskiej S.A., dostępny na stronie internetowej www.bip.poczta-polska.pl/repozytorium/ oraz w każdej placówce Poczty Polskiej;
15. **Role zaufane** – role pełnione przez wyznaczonych członków Personelu w zakresie wskazanym w podrozdziale 4.2.1. Polityki;
16. **Rozporządzenie eIDAS** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE;
17. **Strony Usługi RDE** – podmioty wskazane w podrozdziale 1.3. Polityki;
18. **System identyfikacji elektronicznej** – system identyfikacji elektronicznej, w ramach którego wydaje się środki identyfikacji elektronicznej osobom fizycznym lub prawnym, lub osobom fizycznym reprezentującym osoby prawne;

19. **System RDE** – wszystkie elementy organizacyjne i techniczne zapewniające funkcjonowanie Usługi RDE;
20. **Środek identyfikacji elektronicznej** – materialna lub niematerialna jednostka zawierająca dane identyfikujące osobę i używana do celów uwierzytelniania dla usługi online;
21. **Usługa zaufania** – świadczona za wynagrodzeniem usługa elektroniczna obejmująca czynności wskazane w art. 3 pkt 16 lit. a-c Rozporządzenia eIDAS;
22. **Ustawa** – ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej.

1.3. Definicje Stron Usługi RDE

Nazwa strony	Opis
Dostawca Usługi RDE	Poczta Polska będąca samodzielnym dostawcą Usług RDE
Dostawca usługi identyfikacji elektronicznej	Dostawca środka identyfikacji elektronicznej w ramach notyfikowanego krajowego schematu identyfikacji elektronicznej zapewniający klientom usługi możliwość identyfikacji i uwierzytelnienia
Techniczny dostawca rozwiązania usługi RDE	PPUC z siedzibą w Warszawie, funkcjonująca pod marką Envelo
Klient	Osoba fizyczna, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, będąca nadawcą lub odbiorcą przesyłki elektronicznej
Strona ufająca	Osoba fizyczna, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, polegająca na zaufaniu do usługi zaufania rejestrowanego doręczenia elektronicznego opisanego w Polityce
Administracja publiczna	Organy administracji publicznej (państwowej lub samorządowej) wykorzystujące Usługę RDE do kontaktu z obywatelem, przedsiębiorcami, jak również w komunikacji pomiędzy różnymi jednostkami administracji publicznej
Inny dostawca usługi zaufania	Inny niż Poczta Polska dostawca usługi zaufania, (np. kwalifikowanej usługi elektronicznego znacznika czasu lub usługi zaawansowanej pieczęci elektronicznej)

1.4. Zakres Usługi RDE

1. Usługa RDE może być realizowana przez jednego Dostawcę usług zaufania lub też może umożliwiać doręczenie dzięki współpracy wielu Dostawców usług zaufania.
2. Wszyscy Kwalifikowani dostawcy usług zaufania współpracujący z Pocztą Polską są zobowiązani spełniać wymagania bezpieczeństwa wynikające z Polityki.

1.5. Podstawowe elementy Usługi RDE

1. Usługa RDE składa się z następujących elementów: wysłania Przesyłki, odbioru Przesyłki i wystawienia dowodów dokonanych czynności:
   1) wysłanie Przesyłki obejmujące następujące kroki:
      a) identyfikację i uwierzytelnienie Klienta realizującego nadanie Przesyłki w Systemie RDE,
      b) przekazanie przez Klienta Przesyłki do nadania przez dostawcę Usługi RDE,
      c) wystawienie dowodu nadania przez dostawcę Usługi RDE,
   2) odbiór Przesyłki obejmujący następujące kroki:
      a) przekazanie przez Dostawcę Usługi RDE do Klienta w roli odbiorcy informacji o nowej Przesyłce i prośba o akceptację przyjęcia Przesyłki,
      b) akceptacja lub odmowa akceptacji przez Klienta Przesyłki, przy czym odmowa akceptacji Przesyłki może także zostać zrealizowana poprzez zaniechanie jej odbioru,
      c) wystawienie dowodu preawizacji Przesyłki przez Dostawcę Usługi RDE,
      d) identyfikacja i uwierzytelnienie przez System RDE Klienta przed odbiorem Przesyłki,
      e) przekazanie Przesyłki poza Usługę RDE do odbiorcy,
   3) wystawienie dowodów:
      a) nadania Przesyłki (w tym dokładny czas nadania) – dostępny dla nadawcy,
      b) preawizacji – dostępny dla nadawcy i odbiorcy,
      c) odbioru Przesyłki (w tym dokładny czas odbioru) – dostępny dla nadawcy i odbiorcy (generowany także w przypadku zaniechania odbioru).
2. Każda zmiana danych niezbędna do celów wysłania lub otrzymania danych jest wyraźnie wskazana nadawcy (przed wysłaniem) i adresatowi (przed odbiorem) danych w postaci komunikatu elektronicznego.
3. Dowody w zakresie nadania, preawizacji oraz odbioru Przesyłki są zabezpieczone pieczęcią elektroniczną oraz znakowane czasem. Poczta Polska udostępnia Klientom dowody wytworzone w procesie świadczenia Usługi RDE przez okres nie krótszy niż 24 miesiące od momentu ich wytworzenia.

4. Niezależnie od utraty danych z powodów technicznych lub innych, Poczta Polska zapewnia utrzymanie dokumentów i danych, wynikających z art. 17 Ustawy, przez okres 20 lat od momentu ich wytworzenia.

2. Administracja i repozytorium

2.1. Administracja Polityką

1. Poczta Polska wskazuje Z-cę Dyrektora CTC ds. Cyfryzacji, jako podmiot odpowiedzialny za administrowanie Polityką.
2. Każdorazowa zmiana Polityki wymaga podjęcia uchwały przez Zarząd Poczty Polskiej. Z chwilą dokonania zmian, w Metryce dokumentu wskazywany jest aktualny status danej wersji Polityki i data, od której obowiązuje.
3. Za ocenę aktualności i przydatności Polityki odpowiada Z-ca Dyrektora CTC ds. Cyfryzacji.
4. W ramach świadczenia Usługi RDE, Poczta Polska dokonuje przeglądów stosowanych praktyk zgodnie z prowadzoną procedurą zarządzania ryzykiem.

2.2. Repozytorium i publikacja dokumentu

1. Repozytorium jest centralną bazą danych zawierającą informacje o:
   1) aktualnej i obowiązującej wersji Polityki,
   2) historycznych wersjach Polityki,
   3) regulaminie Usługi RDE,
   4) innych dokumentach przeznaczonych do publikacji na podstawie Polityki, jeśli takie wskazano.
2. Dokumenty umieszczone w repozytorium są publicznie dostępne pod adresem https://bip.poczta-polska.pl/repozytorium/.
3. Wszelkie zmiany Polityki są archiwizowane, a ich zmienione wersje publikowane na bieżąco (każdorazowo, gdy zostaną uaktualnione lub zmienione).
4. Wszystkie informacje publikowane w repozytorium są ogólnie dostępne. Informacje te są zabezpieczone przed nieautoryzowanym zmienianiem, dodawaniem i usuwaniem oraz są przechowywane z zachowaniem kopii zapasowych.

3. Identyfikacja i uwierzytelnienie

1. Poczta Polska w ramach Usługi RDE korzysta z zewnętrznego procesu identyfikacji elektronicznej, w ramach Usługi RDE nie jest wydawany środek uwierzytelniający.
2. Każdy adres do doręczeń elektronicznych zapewnia jednoznaczną identyfikację nadawcy i odbiorcy. Usługa RDE dopuszcza równoległe funkcjonowanie podstawowego adresu wraz z adresami funkcjonującymi u innych dostawców Usługi RDE. W zakresie adresacji Usługa RDE umożliwia korzystanie ze wspólnej infrastruktury adresowej udostępnionej przez ministra właściwego ds. informatyzacji na podstawie właściwych przepisów.

3. Usługa RDE umożliwia mapowanie adresu do doręczeń elektronicznych, w szczególności w zakresie akceptacji wiadomości pochodzących od innych dostawców, a także wiadomości doręczanych w ramach krajowych ram dla doręczeń.
4. W ramach Usługi RDE dopuszcza się następujące sposoby identyfikacji i uwierzytelnienia:
   1) w oparciu o Krajowy Schemat Identyfikacji zgodnie z art. 21a Ustawy, w szczególności Środki identyfikacji elektronicznej wchodzące w skład Krajowego Schematu Identyfikacji pozwalające na założenie Profilu Zaufanego („**eGO**"),
   2) w oparciu o zaawansowany podpis elektroniczny lub zaawansowaną pieczęć elektroniczną na postawie certyfikatów rozpoznawanych przez Usługę RDE tzn. certyfikat kwalifikowany, certyfikat podpisu osobistego oraz inne certyfikaty wydane na podstawie polityki certyfikacji zgodnej z profilem NCP+ określonym standardem ETSI EN 319411-2,
   3) w oparciu o środek identyfikacji elektronicznej uznany na poziomie krajowym, w szczególności środek stosowany do uwierzytelniania w systemie teleinformatycznym banku krajowego lub innego przedsiębiorcy, spełniającym warunki ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne.
5. Identyfikacja elektroniczna przeprowadzana jest za każdym razem przed nadaniem lub doręczeniem Przesyłki. Jeżeli identyfikacja odbiorcy opiera się na zaawansowanym podpisie elektronicznym, weryfikacja podpisu poprzedza przekazanie Przesyłki.
6. Poczta Polska, wykorzystując do identyfikacji elektronicznej zewnętrzne systemy identyfikacji elektronicznej, zapewnia, że systemy te są uznane krajowo oraz oferują identyfikację bezpieczeństwa na średnim poziomie wiarygodności.

4. Zabezpieczenia organizacyjne, operacyjne i fizyczne

1. Poczta Polska posiada wewnętrzny dokument dotyczący polityki bezpieczeństwa informacji, który określa podstawowe zasady zarządzania bezpieczeństwem informacji w zakresie Usługi RDE.
2. Wewnętrzny dokument dotyczący polityki bezpieczeństwa informacji jest komunikowany każdej osobie pełniącej Rolę zaufaną w zakresie Usługi RDE świadczonej przez Pocztę Polską, zaś Poczta Polska jest zobowiązana do dokumentowania oświadczeń tych osób o zobowiązaniu się do przestrzegania zasad i wytycznych ujętych w ww. dokumencie.

4.1. Zabezpieczenia fizyczne

4.1.1. Lokalizacja i budynki

Systemy teleinformatyczne wykorzystywane do świadczenia Usługi RDE mieszczą się w dwóch niezależnych lokalizacjach (centrum podstawowym i centrum zapasowym).

4.1.2. Dostęp fizyczny

1. Fizyczny dostęp do budynku oraz pomieszczeń wykorzystywanych w ramach świadczenia Usługi RDE jest kontrolowany przez pracowników ochrony oraz nadzorowany przez elektroniczny system zabezpieczenia technicznego.
2. Ochrona fizyczna budynków funkcjonuje 24 godziny na dobę.
3. Pomieszczenia, w których znajduje się system teleinformatyczny, w tym także pomieszczenia, w których znajduje się bezpieczny moduł kryptograficzny, wyposażone są w system kontroli dostępu do pomieszczeń oraz system sygnalizacji włamania i napadu.
4. Dostęp do pomieszczeń wykorzystywanych w ramach świadczenia Usługi RDE posiadają tylko osoby upoważnione.
5. Weryfikacja uprawnień dostępu do pomieszczeń realizowana jest w oparciu o elektroniczny system kontroli dostępu umożliwiający identyfikację i rozliczalność osób upoważnionych.

4.1.3. Bezpieczeństwo środowiskowe

1. W przypadku zaniku zasilania podstawowego System RDE przechodzi na zasilanie awaryjne poprzez UPS, czyli urządzenie, którego funkcją jest nieprzerwane zasilanie urządzeń elektronicznych Systemu RDE.
2. Środowisko pracy w pomieszczeniach systemu komputerowego kontrolowane jest w sposób ciągły i niezależny od innych pomieszczeń. Ponadto wszystkie pomieszczenia są klimatyzowane.
3. Czujniki zalania są zainstalowane w pomieszczeniach serwerowni. Alarmy o zalaniu przekazywane są do ochrony i administratora budynku, którzy zawiadamiają odpowiednie służby miejskie, Inspektora bezpieczeństwa oraz Administratora systemu.
4. System ochrony przeciwpożarowej, zainstalowany w pomieszczeniach systemu komputerowego, spełnia wymogi stosownych przepisów i norm przeciwpożarowych. W serwerowni zainstalowano urządzenia gaśnicze (gazowe), które załączają się automatycznie, w przypadku wykrycia pożaru w chronionym obszarze.

4.1.4. Nośniki informacji

Nośniki, na których przechowywane są kopie bezpieczeństwa środowiska kryptograficznego, składowane są w sejfach ognioodpornych. Dostęp do sejfów mają osoby pełniące role Inspektora bezpieczeństwa, Administratora systemu oraz Audytora.

4.1.5. Niszczenie informacji

Papierowe oraz elektroniczne nośniki zawierające informacje, mogące mieć wpływ na bezpieczeństwo Poczty Polskiej, dane osobowe oraz informacje stanowiące tajemnicę pocztową, po upływie okresu przechowywania rejestrowanych i archiwizowanych zdarzeń niszczone są w urządzeniach specjalnie do tego przeznaczonych.

4.1.6. Kopie bezpieczeństwa

1. Zapisy zdarzeń są kopiowane zgodnie z harmonogramem tworzenia kopii bezpieczeństwa systemu teleinformatycznego. Kopie te przechowywane są w sejfach znajdujących się w centrum podstawowym.
2. Czynności tworzenia kopii zapasowych wykonywane są przez Operatora systemu w obecności Inspektora bezpieczeństwa.

4.2. Zabezpieczenia organizacyjne

4.2.1. Role zaufane

1. Osoby sprawujące nadzór nad Systemem RDE pełnią określone Role zaufane, które zaprezentowano w poniższej tabeli.

Nazwa Roli zaufanej	Zakres głównych obowiązków
Z-ca Dyrektora CTC ds. Cyfryzacji	▪ Zapewnienie prawidłowej organizacji i funkcjonowania Usługi RDE. Wdrożenie/Wdrażanie postanowień Polityki. ▪ Zapewnienie zgodności Usługi RDE z prawem oraz standardami normalizacyjnymi. ▪ Nadzorowanie zapewnienia ciągłości działania oraz zapewnienie realizacji planu zakończenia działalności.
Kierownik Działu odpowiedzialny za systemy usług zaufania	▪ Zarządzanie działem i nadzorowanie jego funkcjonowania. ▪ Zapewnienie prawidłowej organizacji i funkcjonowania Systemu RDE. ▪ Realizacja kierunków rozwoju usług. ▪ Utrzymanie aktualności planu zakończenia działalności.
Operator systemu	▪ Instalowanie, konfigurowanie i zarządzanie systemami oraz sieciami teleinformatycznymi wykorzystywanymi na potrzeby świadczenia Usługi RDE. ▪ Dbałość o operacyjne aspekty świadczenia Usługi RDE. ▪ Wykonywanie procedur i instrukcji operacyjnych. ▪ Realizacja procedur utrzymania Systemu RDE.
Administrator systemu	▪ Zapewnienie współpracy z dostawcą (dostawcami), w szczególności z PPUC i umiejscowionymi u tego dostawcy Operatorami systemu. ▪ Operacyjne czynności w zakresie zarządzania kluczami.
Inspektor bezpieczeństwa	▪ Zapewnienie bezpieczeństwa procesu w ramach świadczonej Usługi RDE. ▪ Wdrażanie i realizacja postanowień wewnętrznego dokumentu dotyczącego polityki bezpieczeństwa informacji, w tym m.in.: ✓ zapewnienie zarządzania ryzykiem, ✓ nadzorowanie procesu zarządzania incydentami, ✓ nadzorowanie bezpieczeństwa fizycznego, bezpieczeństwa sieci oraz zarządzania ciągłością działania, ✓ zarządzanie uprawnieniami w zakresie Usługi RDE.

Audytor	▪ Przeglądanie archiwów i dzienników zdarzeń Usługi RDE. ▪ Analizowanie zdarzeń i incydentów dotyczących Usługi RDE. ▪ Rekomendowanie działań naprawczych i profilaktycznych. ▪ Kontrola wdrożonych mechanizmów i środków bezpieczeństwa.
Koordynator ds. wdrożenia eUsług	▪ Koordynowanie działań dotyczących Usługi RDE.
Inspektor ds. weryfikowania tożsamości	▪ Odpowiedzialność za proces weryfikacji tożsamości nadawcy i odbiorcy i zgodność jego rzeczywistego przebiegu z przyjętymi założeniami.

2. Wymienione w ust. 1 role i obowiązki związane z bezpieczeństwem (Inspektor bezpieczeństwa oraz Audytor) zostały również szczegółowo określone w wewnętrznym dokumencie dotyczącym polityki bezpieczeństwa informacji.
3. Poczta Polska deklaruje, że opisany zakres obowiązków dokumentuje się w opisie danego stanowiska, jak również w wewnętrznym dokumencie opisującym szczegółowo zakres odpowiedzialności dla poszczególnej Roli zaufanej w Systemie RDE.

4.2.2. Role zaufane podlegające separacji obowiązków

1. Role zaufane wyodrębnione w ramach Personelu zapobiegają nadużyciom, przy korzystaniu z Systemu RDE.
2. Każdej osobie odpowiedzialnej za eksploatację Systemu RDE wykorzystywanego do świadczenia Usługi RDE przydzielono tylko takie prawa, które wynikają z pełnionej przez nią Roli zaufanej i ponoszonej z tego tytułu odpowiedzialności.
3. Rola Inspektora bezpieczeństwa nie może być łączona z rolą Administratora systemu ani z rolą Operatora systemu. Rola Audytora nie może być łączona z żadną z pozostałych Ról zaufanych.

4.2.3. Zarządzanie incydentami

1. Poczta Polska na żądanie ministra właściwego ds. informatyzacji, z zachowaniem przepisów o ochronie informacji prawnie chronionych, udziela informacji lub udostępnia dokumenty, które są bezpośrednio związane ze świadczonymi Usługami zaufania lub mają wpływ na świadczone Usługi zaufania, w tym dotyczą zarządzania incydentami związanymi z Usługą RDE.
2. Poczta Polska bez zbędnej zwłoki, a w każdym razie nie później niż 24 godziny od otrzymania informacji o wystąpieniu incydentu, zawiadamia ministra właściwego ds. informatyzacji, w stosownych przypadkach, inne właściwe podmioty, o wszelkich przypadkach naruszenia bezpieczeństwa lub utraty integralności, które mają znaczący wpływ na świadczoną Usługę zaufania lub przetwarzane w jej ramach dane osobowe.
3. Powyższe obowiązki notyfikacyjne pozostają bez uszczerbku dla obowiązków notyfikacyjnych Poczty Polskiej wynikających z odrębnych przepisów, w tym

w szczególności Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) oraz ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

4. W ramach świadczenia Usługi RDE istnieje także procedura wewnętrzna regulująca zarządzanie incydentami.

4.2.4. Zarządzanie ryzykiem

Zarządzanie ryzykiem prowadzone jest zgodnie z ustanowioną w Poczcie Polskiej procedurą zarządzania ryzykiem, w celu dostosowania zabezpieczeń techniczno-organizacyjnych do zidentyfikowanych zagrożeń dla Usługi RDE.

4.2.5. Nadzór nad Personelem pełniącym Role zaufane

4.2.5.1. Kwalifikacje, doświadczenie, upoważnienia

Osoby uczestniczące w świadczeniu Usługi RDE, pełniące Role zaufane, posiadają odpowiednie kwalifikacje przewidziane dla Kwalifikowanych dostawców usług zaufania, w szczególności wiedzę i umiejętności z zakresu infrastruktury klucza publicznego oraz przetwarzania danych osobowych, a ponadto:

1) posiadają pełną zdolność do czynności prawnych,
2) posiadają minimum wykształcenie średnie,
3) zobowiązały się do nieujawniania informacji wrażliwych, z punktu widzenia bezpieczeństwa dostawcy Usługi RDE lub poufności danych Klienta, wynikających z wewnętrznego dokumentu dotyczącego polityki bezpieczeństwa informacji,
4) nie wykonują obowiązków, które mogą doprowadzić do konfliktu interesów pomiędzy urzędem znacznika czasu a działającymi w jego imieniu punktami rejestracji,
5) zapoznały się z wewnętrznymi procedurami Poczty Polskiej dotyczącymi Usługi RDE,
6) zostały poinformowane o odpowiedzialności karnej w zakresie związanym ze świadczeniem Usług zaufania,
7) zostały przeszkolone w zakresie zasad świadczenia Usług zaufania, w tym: wdrożonych procedur i polityk oraz związanych z nimi zasad bezpieczeństwa.

4.2.5.2. Weryfikacja Personelu

1. Przed powierzeniem Personelowi którejkolwiek z Ról zaufanych przeprowadzana jest co najmniej weryfikacja:
   1) świadectwa pracy z poprzednich miejsc zatrudnienia (w przypadku nowej osoby),
   2) dyplomu i świadectwa potwierdzających wykształcenie tej osoby,
   3) kwalifikacji i doświadczenia zawodowego.
2. Weryfikacja przeprowadzana jest z poszanowaniem wymogów określonych we właściwych przepisach w zakresie przetwarzania danych osobowych.

4.2.5.3. Szkolenia

1. Osoby pełniące Role zaufane w ramach Usługi RDE przechodzą cykl szkoleń dotyczących:
   1) zasad określonych w Polityce,
   2) zasad zawartych w dokumentacji przypisanej Roli zaufanej, którą dana osoba pełni i zakresu obowiązków, które będzie wykonywała,
   3) ochrony danych osobowych i ochrony informacji,
   4) infrastruktury klucza publicznego,
   5) zasad i mechanizmów zabezpieczeń stosowanych w Usłudze RDE,
   6) oprogramowania systemu komputerowego Usługi RDE,
   7) procedur realizowanych po awariach lub katastrofach Systemu RDE,
   8) zagrożeń i aktualnych praktyk bezpieczeństwa.
2. Szkolenia, o których mowa w ust. 1, są powtarzane co najmniej raz na dwa lata oraz w zależności od potrzeb zawsze wtedy, gdy nastąpiły istotne zmiany w świadczeniu Usługi RDE przez Pocztę Polską.

4.2.5.4. Sankcje z tytułu nieuprawnionych działań

1. W przypadku wykrycia nieuprawnionego działania lub podejrzenia o takie działanie ze strony Personelu, Administrator systemu w porozumieniu z Inspektorem bezpieczeństwa może w pierwszej kolejności zablokować dostęp do Systemu RDE sprawcy takiego zdarzenia.
2. Dalsze postępowanie przeprowadzane jest w porozumieniu z Zarządem Poczty Polskiej i może prowadzić do złożenia zawiadomienia o możliwości popełnienia przestępstwa.
3. Osoby pełniące Role zaufane oraz wszyscy zewnętrzni dostawcy zostali poinformowani o sankcjach karnych wynikających z Ustawy.

4.2.5.5. Pracownicy kontraktowi

1. Dopuszcza się zatrudnianie pracowników kontraktowych, w celu zapewnienia niezbędnych zasobów w kontekście świadczenia Usługi RDE.
2. Zakres odpowiedzialności osób fizycznych świadczących osobiście usługi na rzecz Poczty Polskiej lub PPUC w oparciu o umowę cywilnoprawną (umowę o dzieło, umowę zlecenia, umowę o świadczenie usług) został zdefiniowany w stosownych umowach dotyczących współpracy.

4.2.5.6. Dokumentacja dla Personelu pełniącego Role zaufane

Poczta Polska umożliwia członkom swojego Personelu pełniącym Role zaufane dostęp do następujących dokumentów:

1) Polityki,
2) procedur eksploatacyjnych (tylko dla Ról zaufanych) w zakresie obsługi Systemu RDE,
3) stosowanych formularzy wniosków,

4) niezbędnych wyciągów z dokumentacji (właściwej dla pełnionej Roli zaufanej), w tym procedur awaryjnych,
5) zakresu obowiązków i uprawnień wynikających z pełnionej Roli zaufanej.

4.3. Bezpieczna eksploatacja

4.3.1. Rejestrowanie zdarzeń

1. W ramach Usługi RDE rejestrowaniu podlegają w szczególności następujące zdarzenia:
   1) zdarzenia bezpośrednio związane ze świadczeniem Usług zaufania, a w szczególności:
      a) dowody na to, że zasady i warunki świadczenia Usługi RDE zostały zaakceptowane przez Klienta,
      b) czynności systemowe dotyczące dostępu do systemów informatycznych, korzystania z systemów informatycznych i zgłoszeń serwisowych,
      c) czynności związane z identyfikacją i uwierzytelnieniem Klientów Usługi RDE,
      d) czynności związane z obsługą Klientów, w tym dowody w zakresie m.in. wysłania i odbioru Przesyłek,
   2) logi systemowe z serwerów i stacji roboczych wchodzących w skład Systemu RDE,
   3) zdarzenia związane z obsługą techniczną systemu, tj.: błędy i alarmy, rejestr wprowadzanych zmian w systemie,
   4) zdarzenia związane z bezpieczeństwem, w tym zmiany związane z wewnętrznym dokumentem dotyczącym polityki bezpieczeństwa informacji, uruchamianiem i zamykaniem Systemu RDE, awariami Systemu RDE i awariami sprzętu, działaniami zapory i routera oraz próbami dostępu do Systemu RDE.
2. Ponadto Poczta Polska zapewnia przechowywanie dowodów w postaci raportów z prowadzonych testów bezpieczeństwa, audytów konfiguracji oraz testów penetracyjnych.
3. Logi są zabezpieczone przed modyfikacją, podlegają procedurom tworzenia kopii zapasowych oraz są archiwizowane.
4. Dostęp do archiwów mają: Audytor, Z-ca Dyrektora CTC ds. Cyfryzacji oraz osoby upoważnione przez Z-cę Dyrektora CTC ds. Cyfryzacji.
5. Rejestry zdarzeń zapisywane są w formie elektronicznej. Rekordy zawierają: identyfikator zdarzenia, datę i czas wystąpienia zdarzenia, typ i szczegółowy opis zdarzenia. Stary rejestr po zarchiwizowaniu jest usuwany z dysku, zgodnie z wewnętrzną polityką archiwizacji.
6. Zapisy rejestrowanych zdarzeń przechowywane są w plikach na dysku systemowym, przez okres przynajmniej 24 miesięcy.
7. Czas wykorzystywany do rejestrowania zdarzeń zgodnie z wymaganiami w rejestrze zdarzeń jest synchronizowany z UTC, co najmniej raz dziennie.

4.3.2. Tworzenie kopii zapasowych i odtwarzanie

1. Zapisy zdarzeń są kopiowane zgodnie z harmonogramem tworzenia kopii bezpieczeństwa Systemu RDE. Kopie te przechowywane są w sejfach znajdujących się w centrum podstawowym.
2. Czynności tworzenia kopii zapasowych wykonywane są przez Operatora systemu w obecności Inspektora bezpieczeństwa.

4.3.3. Archiwizacja zdarzeń

1. W ramach Usługi RDE archiwizacji podlegają w szczególności:
   1) dane identyfikacyjne Klientów lub Personelu pełniącego Role zaufane,
   2) dane uwierzytelniające Klientów lub Personelu pełniącego Role zaufane,
   3) dowód, że tożsamość nadawcy została pierwotnie zweryfikowana,
   4) logi operacji Usługi RDE, weryfikacji tożsamości nadawcy i odbiorcy oraz komunikacji,
   5) dowody weryfikacji tożsamości odbiorcy przed wysyłką/przekazaniem Przesyłki,
   6) dowody na to, że Przesyłka nie została zmodyfikowana podczas transmisji,
   7) odniesienie do lub przesłanie całej Przesyłki,
   8) tokeny znaczników czasu odpowiadające dacie i godzinie wysyłania, przekazywania oraz modyfikowania Przesyłki, stosownie do przypadku,
   9) Polityka oraz jej historyczne wersje,
   10) inne dokumenty umieszczone w repozytorium zgodnie z zapisami Polityki.
2. Archiwum zawiera również wszelkie dokumenty papierowe, związane ze świadczeniem Usługi RDE, których okres przechowywania wynosi 20 lat zgodnie z art. 17 Ustawy, z zastrzeżeniem art. 20 ust. 1 Ustawy.
3. Poczta Polska zapewnia poufność, integralność i dostępność tworzonych rejestrów zdarzeń.
4. Zapisy dotyczące funkcjonowania Usługi RDE są udostępniane, jeśli jest to wymagane, w celu udokumentowania prawidłowego działania Usługi RDE dla celów postępowania sądowego.

4.4. Zakończenie działalności w zakresie Usługi RDE lub przekazanie zadań przez Pocztę Polską

1. Poczta Polska, mając na uwadze redukcję wpływu skutków podjęcia potencjalnej decyzji o zakończeniu świadczenia działalności w zakresie świadczenia Usługi RDE, planuje w szczególności spełnienie obowiązku odpowiednio wczesnego poinformowania o tym organu nadzoru, wszystkich Stron Usługi RDE, kontrahentów i partnerów, z którymi Poczta Polska jest związana umowami, na których zakończenie świadczenia Usługi RDE będzie miało wpływ, oraz przekazania dokumentów i danych związanych ze świadczeniem Usług zaufania organowi nadzoru.

2. Szczegółowy sposób postępowania w przypadku zakończenia działalności w zakresie świadczenia Usługi RDE przez Pocztę Polską określa Plan zakończenia działalności usługi rejestrowanego doręczenia elektronicznego w Poczcie Polskiej S.A.
3. Organ nadzoru jest informowany o planie zakończenia działalności w zakresie świadczenia Usługi RDE przez Pocztę Polską oraz każdorazowo o każdej jego zmianie.
4. Poczta Polska zobowiązuje się do wykonania następujących czynności:
   1) zapewnienia ciągłości pełnienia roli dostawcy Usługi RDE nie dłużej niż 3 miesiące od dnia poinformowania organu nadzoru o zamiarze zaprzestania bądź niemożności pełnienia roli podmiotu dostawcy Usługi RDE,
   2) utrzymania dokumentów i danych wynikających z treści Polityki oraz danych wymaganych do weryfikacji poprawności świadczenia Usług zaufania, w tym dokumentów i danych przez okres 20 lat od ich wytworzenia,
   3) unieważnienia wszystkich wydanych pełnomocnictw do podpisywania umów o świadczenie Usługi RDE w imieniu Poczty Polskiej, nie później niż na dzień zakończenia działalności w zakresie świadczenia Usługi RDE,
   4) przekazania do zniszczenia lub wycofania kluczy urzędu Usług zaufania i ich kopii zapasowych, w przypadku, gdy nie przewiduje się dalszego wykorzystania tych danych lub w przypadku unieważnienia certyfikatu Dostawcy usług zaufania powiązanego z tymi usługami.

5. Zabezpieczenia techniczne

1. Dane przesyłane pomiędzy stacjami roboczymi a serwerami muszą być szyfrowane, zaś zabezpieczenia Systemu RDE muszą spełniać wymogi aktów normatywnych obowiązujących w chwili świadczenia Usługi RDE.
2. Dane muszą być zabezpieczone przed utratą, modyfikacją, utratą integralności i nieuprawnionym dostępem.

5.1. Zabezpieczenia sprzętu komputerowego

1. Wymagania techniczne określone w niniejszym rozdziale odnoszą się do kontroli zabezpieczeń pojedynczego komputera oraz zainstalowanego na nim oprogramowania w ramach Systemu RDE.
2. Funkcje zabezpieczające systemów komputerowych są realizowane na poziomie systemu operacyjnego, aplikacji oraz zabezpieczeń fizycznych.
3. Pracownik, który pełni Rolę zaufaną, zobowiązany jest do blokowania swojej stacji roboczej zawsze, jeśli pozostaje ona poza jego nadzorem.
4. Komputery pracujące w Systemie RDE wyposażone są w następujące funkcje zabezpieczające:

1) obligatoryjnie uwierzytelnione rejestrowanie się na poziomie systemu operacyjnego i aplikacji (w przypadkach, gdy jest to istotne, np. z punktu widzenia pełnionej Roli zaufanej),
2) uznaniową kontrolę dostępu,
3) możliwość prowadzenia audytu zabezpieczeń,
4) udostępnianie tylko osobom pełniącym Role zaufane,
5) wymuszanie separacji obowiązków wynikających z pełnionych Ról zaufanych,
6) wymuszanie wylogowania Personelu pełniącego Role zaufane po okresie bezczynności,
7) identyfikację i uwierzytelnienie Ról zaufanych oraz pełniących je osób,
8) kryptograficzną ochronę sesji wymiany informacji oraz zabezpieczenie baz danych,
9) archiwizowanie danych dla potrzeb audytu,
10) bezpieczną ścieżkę, pozwalającą na wiarygodną identyfikację i uwierzytelnienie Ról zaufanych oraz pełniących je osób,
11) mechanizm odtwarzania kluczy (tylko w przypadku modułów kryptograficznych) oraz systemu operacyjnego i aplikacji,
12) mechanizm monitorowania i alarmowania w przypadku wystąpienia zdarzeń nieautoryzowanego dostępu do zasobów komputera.

5.2. Cykl życia zabezpieczeń technicznych

1. Nadzór nad wprowadzaniem modyfikacji lub zmian w Systemie RDE sprawuje Inspektor bezpieczeństwa. Zatwierdza on konfigurację Systemu RDE oraz wszelkie zmiany oprogramowania i sprzętu.
2. Testy nowych wersji oprogramowania lub wykorzystanie do tego celu istniejących baz danych odbywa się w środowisku testowym. Zasady stosowane przez Pocztę Polską podczas przeprowadzania tych testów gwarantują nieprzerwaną pracę Systemu RDE, integralność jego zasobów oraz zachowanie poufności danych.
3. Kontrola zarządzania bezpieczeństwem ma na celu takie nadzorowanie funkcjonowania Systemu RDE, które daje pewność, że system ten pracuje prawidłowo i jego funkcje są zgodne z zaplanowaną i zrealizowaną konfiguracją.
4. Mimo że prace administracyjne oraz zmiany w Systemie RDE są rejestrowane, to każda z wprowadzonych zmian wymaga dodatkowo zweryfikowania i akceptacji przez przynajmniej dwie osoby: Inspektora bezpieczeństwa oraz Administratora systemu.
5. System kontroli zmiany informuje uprawnionych pracowników o wystąpieniu modyfikacji w Systemie RDE i wymaga jej weryfikacji przez osobę inną od tej, która wprowadzała daną zmianę.
6. Aktualna konfiguracja Systemu RDE, jak również modyfikacje i aktualizacje tego systemu są dokumentowane i kontrolowane. Zastosowane w Systemie RDE mechanizmy

pozwalają na ciągłą weryfikację integralności oprogramowania, kontrolę ich wersji, a także uwierzytelnianie i weryfikowanie źródła pochodzenia.

7. Polityka nie narzuca cyklu życia stosowanych zabezpieczeń. Zabezpieczenia są wymieniane w przypadku zaistnienia potrzeby zastosowania innych niż obecnie używane, zmian w regulacjach prawnych lub jeśli są technologicznie przestarzałe i nie odpowiadają bieżącym normom i standardom.

5.3. Zabezpieczenia sieci

1. Nadzór nad bezpieczeństwem sieci Systemu RDE sprawują Administratorzy systemu.
2. Sieć w ramach Usługi RDE podzielono na kilka logicznie odseparowanych segmentów, tj.:
   1) strefę chronioną serwerów, w tym serwerów aplikacji, baz danych, logów,
   2) strefę chronioną stacji Operatorów systemu,
   3) strefę chronioną stacji Administratorów systemu,
   4) strefę chronioną stacji Audytorów,
   5) strefę ograniczonego zaufania z publicznymi serwerami usługowymi.
3. Dla stref, o których mowa w ust. 2, stosuje się zdefiniowane polityki kontroli ruchu sieciowego.
4. Komunikacja ze strefy chronionej do stref publicznych jest zabezpieczona za pomocą skonfigurowanych narzędzi firewall. Dostęp od strony Internetu do każdego z segmentów chroniony jest przy pomocy narzędzi firewall.
5. Cała komunikacja pomiędzy systemami Usługi RDE, zlokalizowanymi w różnych ośrodkach, jest realizowana za pomocą szyfrowanych kanałów, zapewniających identyfikację Stron Usługi RDE oraz zabezpieczenie przed jakąkolwiek ingerencją w treść komunikacji.
6. W usłudze sieciowej wykorzystywane są najnowocześniejsze protokoły i algorytmy do szyfrowania na poziomie warstwy transportowej. Usługi sieciowe korzystają z certyfikatów uwierzytelniania strony internetowej TLS, jeśli dane są wysyłane poza sieciami wewnętrznymi. W szczególności dostęp użytkownika jest realizowany w protokole HTTPS.
7. Szczegółowy zakres połączeń pomiędzy poszczególnymi strefami jest opisany w dokumentacji Systemu RDE i stanowi tajemnicę przedsiębiorstwa Poczta Polska.
8. Na podstawie prowadzonych przeglądów konfiguracji sieci, przeglądów uprawnień kont sieciowych, jak również na podstawie wykonywanych analiz i testów bezpieczeństwa, wszelkie usługi sieciowe oraz konta sieciowe, które nie są używane, są blokowane lub dezaktywowane.
9. Poczta Polska przeprowadza regularnie (nie rzadziej niż raz na 6 miesięcy) skany podatności sieci. Ponadto, zapewnia, że wszelkie działania korygujące wobec zidentyfikowanych luk w zabezpieczeniach są rejestrowane.

10. W przypadku potrzeby zapewnienia wysokiego poziomu dostępności do Usługi RDE, zewnętrzne połączenia sieciowe będą nadmiarowe (redundantne), w przypadku pojedynczej awarii. Decyzje o podjęciu określonych środków bezpieczeństwa podejmowane są na mocy prowadzonych analiz ryzyka, zgodnie z wewnętrzną procedurą. Usługa RDE, łącząc się z innymi dostawcami Usługi RDE oraz systemami zewnętrznymi, zapewnia ich identyfikację w oparciu o mechanizmy sieciowe, tj.: SSL lub IP-SEC.
11. Wszelkie zmiany wprowadzane w urządzeniach sieciowych wymagają wcześniejszej akceptacji Inspektora bezpieczeństwa. Przeprowadzona zmiana zostaje zaimplementowana dopiero po zweryfikowaniu jej przez Administratora systemu, który nie brał bezpośredniego udziału w przygotowywaniu zmiany. W przypadku znaczących zmian w konfiguracji Systemu RDE (po konfiguracji i po aktualizacji lub modyfikacjach infrastruktury lub aplikacji), Poczta Polska zapewnia przeprowadzenie testów penetracyjnych oraz gromadzi dowody z prowadzonych testów.

5.4. Usługa pieczęci elektronicznej

1. Wszystkie Przesyłki są zabezpieczone za pomocą usługi zaawansowanej pieczęci elektronicznej. Integralność Przesyłki i związanych z nią metadanych jest chroniona podczas transmisji, w szczególności w przypadku wymiany z nadawcą/odbiorcą lub między rozproszonymi komponentami Systemu RDE, a także w pamięci masowej. Ochrona integralności jest realizowana poprzez weryfikację pieczęci elektronicznych dla dokumentów nadawanych i odbieranych przez porównanie treści pieczęci.
2. Usługa zaawansowanej pieczęci elektronicznej jest obsługiwana w oparciu o certyfikaty wydane przez Narodowe Centrum Certyfikacji. Wszystkie klucze dla pieczęci elektronicznej są przetrzymywane zgodnie z wymaganiami określonymi w rozdziale 5.6 Zabezpieczenia Kryptograficzne.
3. Poczta Polska zapewnia sprawdzanie poprawności wygenerowanych pieczęci, jeżeli będzie korzystać z usługi zewnętrznego dostawcy usługi kwalifikowanej pieczęci.
4. Poczta Polska zapewnia, iż w takim przypadku, nie rzadziej niż raz na miesiąc, będzie sprawdzać, czy dostawca kwalifikowanej pieczęci elektronicznej znajduje się na liście Kwalifikowanych dostawców usługi zaufania.

5.5. Usługa znakowania czasem

1. Wszystkie dowody wystawiane przez Usługę RDE są znakowane czasem, w oparciu o zewnętrznego kwalifikowanego dostawcę kwalifikowanego znacznika czasu.
2. Poczta Polska zapewnia, iż codziennie dokonuje się kontroli aktualności wpisu dostawcy kwalifikowanego znacznika czasu na liście Kwalifikowanych dostawców usług zaufania.
3. Podpisana jest także umowa z zapasowym kwalifikowanym dostawcą usługi znakowania czasem na wypadek niedostępności podstawowej usługi.

4. Lista kwalifikowanych dostawców, z którymi współpracuje Poczta Polska w zakresie świadczenia Usługi RDE, udostępniona jest na stronie internetowej www.edoreczenia.poczta-polska.pl/dostawcy/.

5.6. Zabezpieczenia kryptograficzne

1. Prowadzony jest rejestr wszystkich kluczy kryptograficznych wraz z informacjami o zakresie ich stosowania oraz osobach odpowiedzialnych za wykorzystywanie i nadzór nad kluczami.
2. Wszelkie klucze kryptograficzne, w tym klucze certyfikatów dla zaawansowanej pieczęci elektronicznej, są przechowywane na inteligentnych urządzeniach kryptograficznych. Usługa pieczętowania jest obsługiwana przez stronę trzecią i połączona za pomocą bezpiecznych łączy. Tylko wartości hash komunikatów są przekazywane do usługi pieczęci.
3. Klucze prywatne Usługi RDE są generowane i przetwarzane w urządzeniach HSM posiadających jeden z certyfikatów:
   1) ISO/IEC 15408 (Common Criteria) dla poziomu EAL4 albo bezpieczniejszego,
   2) ISO/IEC 15408 (Common Criteria) dla poziomu określonego CEN EN 419 221-5:2018 – Protection Profiles for TSP Cryptographic Modules for Trust Services,
   3) FIPS PUB 140-2 dla poziomu 3 albo bezpieczniejszego,
   4) ISO/IEC 19790.

6. Audyt zgodności i inne oceny

Audyty są przeprowadzane w Systemie RDE w celu sprawdzenia zgodności postępowania Poczty Polskiej z wymaganiami nałożonymi na Kwalifikowanych dostawców usług zaufania określonych w Rozporządzeniu eIDAS oraz procedurami i procesami opisanymi w wewnętrznej dokumentacji Systemu RDE.

6.1. Częstotliwość i okoliczności oceny

1. Audyt przeprowadzany jest:
   1) samodzielnie przez Audytorów Usługi RDE,
   2) zgodnie z wewnętrzną procedurą audytu dotyczącą usługi rejestrowanego doręczenia elektronicznego, lub
   3) raz na 2 lata przez zewnętrzną jednostkę oceniającą zgodność na podstawie art. 20 ust. 1 Rozporządzenia eIDAS („**Audyt zewnętrzny**”).
2. Audyt zewnętrzny może być przeprowadzony w każdym momencie na wniosek organu nadzoru w trybie art. 31 Ustawy w związku z art. 17 ust. 4 lit. e i art. 20 ust. 2 Rozporządzenia eIDAS.

6.2. Tożsamość i kwalifikacje audytora

Audyt zewnętrzny przeprowadzany jest przez upoważnioną do tego rodzaju działalności instytucję krajową lub europejską, posiadającą akredytację do przeprowadzania audytów

zgodności dostawców usług zaufania i spełniającą wymogi określone w normie ETSI EN 319 403.

6.3. Związek audytora z audytowaną jednostką

Audytorzy nie mogą prowadzić działalności gospodarczej w zakresie świadczenia Usług zaufania, świadczyć Usług zaufania, być wspólnikami albo akcjonariuszami Dostawcy usług zaufania ani wykonywać obowiązków osoby reprezentującej lub członka rady nadzorczej albo komisji rewizyjnej tego dostawcy, a także pozostawać z tym dostawcą w stosunku pracy, zlecenia lub innym stosunku prawnym o podobnym charakterze.

6.4. Zagadnienia objęte audytem

Do zagadnień objętych audytem należą w szczególności:

1) sprawdzenie wymagań organizacyjno-prawnych wynikających z Rozporządzenia eIDAS i wydanych decyzji wykonawczych do tego rozporządzenia,
2) monitorowanie i zapewnianie zgodności działalności z procedurami i politykami,
3) zabezpieczenia fizyczne,
4) zarządzanie bezpieczeństwem informacji,
5) stosowanie określonych zasad bezpieczeństwa przez Personel pełniący Role zaufane,
6) procedury świadczenia Usługi RDE,
7) zabezpieczenia oprogramowania i dostępu do sieci,
8) rejestry zdarzeń i procedury monitorowania systemu,
9) procedury sporządzania kopii zapasowych oraz ich odtwarzania,
10) realizacja procedur archiwizacji,
11) dokumentowanie zmian parametrów konfiguracyjnych Systemu RDE,
12) przegląd uprawnień w Systemie RDE.

6.5. Działania podejmowane celem usunięcia usterek wykrytych podczas audytu

1. Raporty audytów wewnętrznych i zewnętrznych przekazywane są Zarządowi Poczty Polskiej oraz Z-cy Dyrektora CTC ds. Cyfryzacji.
2. Zarząd Poczty Polskiej powołuje zespół osób w celu przygotowania w terminie określonym w raporcie pisemnego stanowiska Poczty Polskiej wobec wszelkich uchybień wskazanych w raportach, przy jednoczesnym określeniu sposobów i terminu usunięcia usterek. Informacja o usunięciu usterek przekazywana jest audytorowi.
3. W przypadku audytu zleconego przez ministra właściwego ds. informatyzacji, minister po zapoznaniu się z protokołem i zastrzeżeniami oraz wyjaśnieniami zgłoszonymi przez Pocztę Polską powiadamia ten podmiot, o wynikach kontroli i w razie stwierdzenia nieprawidłowości wyznacza termin ich usunięcia, nie krótszy niż 14 dni.

6.6. Informowanie o wynikach audytu

Informacje o wynikach audytu, w postaci raportu z jego przeprowadzenia lub podsumowania z takiego raportu, są udostępniane wyłącznie wewnętrznie upoważnionym osobom, jak: Zarząd Poczty Polskiej, Z-ca Dyrektora CTC ds. Cyfryzacji, Inspektor bezpieczeństwa.

7. Inne postanowienia

7.1. Opłaty

Z tytułu świadczenia Usługi RDE Poczta Polska pobiera opłaty według cennika publikowanego na stronie internetowej www.bip.poczta-polska.pl/repozytorium/.

7.2. Niedyskryminujące zastosowanie

Dzięki wdrożeniu najlepszych rozwiązań w projektowaniu stron internetowych Poczta Polska oferuje Stronom Usługi RDE niedyskryminujący dostęp do Usługi RDE. Strony internetowe zostały przygotowane zgodnie ze standardem WCAG 2.0 (Web Content Accessibility Guidelines).

7.3. Odpowiedzialność finansowa

1. Poczta Polska potwierdza, że zapewniono wystarczające środki finansowe na obsługę Usługi RDE i wypełnienie wszystkich zobowiązań dotyczących Usługi RDE.
2. Wszystkie uzgodnienia, niezbędne do świadczenia Usługi zaufania, z podwykonawcami, partnerami outsourcingowymi i stronami trzecimi, podlegają umowom i regulacjom obowiązującym w tym zakresie w Poczcie Polskiej.
3. Poczta Polska posiada ubezpieczenie odpowiedzialności cywilnej zgodne z wymaganiami Rozporządzenia Ministra Rozwoju i Finansów z dnia 19 grudnia 2016 r. w sprawie obowiązkowego ubezpieczenia odpowiedzialności cywilnej kwalifikowanego dostawcy usług zaufania.

7.4. Poufność informacji

1. Poczta Polska i osoby w niej zatrudnione bądź podmioty dokonujące czynności operacyjno-technicznych, w ramach obsługi Systemu RDE, są obowiązane do zachowania tajemnicy przedsiębiorstwa wszelkich informacji powziętych w trakcie zatrudnienia lub wykonywania czynności jak powyżej także po ustaniu okresu zatrudnienia bądź umocowania do ich wykonywania. Szczegółowy zakres tajemnicy przedsiębiorstwa określony jest w oddzielnych wewnętrznych aktach prawnych Poczty Polskiej. W szczególności dotyczy to:
   1) informacji wpływającej od/do Klientów Usługi RDE,
   2) zapisów transakcji systemowych (zarówno w całości, jak też w postaci danych do przeglądu kontrolnego transakcji, tzw. rejestrów transakcji systemowych),
   3) raportów audytu wewnętrznego oraz zewnętrznego,
   4) informacji o przedsięwziętych środkach zabezpieczających sprzęt oraz oprogramowanie,

5) informacji o administrowaniu Usługami zaufania oraz projektowanymi zmianami w tym zakresie.

7.5. Ochrona danych osobowych

Poczta Polska przetwarza dane osobowe (w szczególności dane Klientów Usługi RDE) zgodnie z obowiązującymi w tym zakresie przepisami prawa oraz wewnętrzną dokumentacją ochrony danych osobowych. Informacje na temat przetwarzania danych osobowych są dostępne w Regulaminie.

7.6. Prawo do własności intelektualnej

Prawa autorskie do Polityki posiada Poczta Polska. Polityka może być wykorzystywana wyłącznie w celu korzystania z oferowanych Usług zaufania. Wszelkie inne zastosowania, w tym wykorzystanie całości lub fragmentu dokumentu, wymaga uprzedniej pisemnej zgody Poczty Polskiej (pod rygorem nieważności), z tym że Poczta Polska wyraża zgodę na powielanie i publikowanie w całości Polityki ze wskazaniem jej źródła.

7.7. Zgodność z obowiązującym prawem

Funkcjonowanie Poczty Polskiej w zakresie świadczenia Usługi RDE oparte jest na zasadach zawartych w Polityce oraz obowiązujących na terytorium Polski przepisach prawa.

7.8. Zobowiązania i gwarancje

7.8.1. Zobowiązania Poczty Polskiej

1. Poczta Polska gwarantuje, że:
   1) postępuje zgodnie z prawem, a w szczególności nie narusza postanowień Rozporządzenia eIDAS, Ustawy wraz z przepisami wykonawczymi oraz nie narusza praw autorskich i licencyjnych stron trzecich,
   2) świadczone Usługi zaufania są zgodne z powszechnie akceptowanymi normami i standardami, m.in.:
      a) ETSI EN 319 401,
      b) ETSI EN 319 521,
   3) zatrudnia osoby pełniące Role zaufane, które posiadają wiedzę, kwalifikacje i doświadczenie odpowiednie do pełnienia funkcji związanych z Usługami zaufania, w tym w szczególności obejmujące dziedziny:
      a) automatycznego przetwarzania danych w sieciach i systemach teleinformatycznych,
      b) mechanizmów zabezpieczania sieci i systemów teleinformatycznych,
      c) kryptografii, pieczęci elektronicznych,
      d) sprzętu i oprogramowania stosowanego do elektronicznego przetwarzania danych.
2. Wszystkie zegary funkcjonujące w ramach Usługi RDE są synchronizowane z międzynarodowym wzorcem czasu UTC, z dokładnością do 1 sekundy.

7.8.2. Zobowiązania zewnętrznych podmiotów

1. Celem realizacji Usług zaufania Poczta Polska współpracuje z PPUC, która jest dostawcą technicznego rozwiązania wykorzystywanego do świadczenia Usługi RDE oraz operatorem Systemu RDE. PPUC na podstawie umowy zawartej z Pocztą Polską zobowiązana jest do przestrzegania wymagań wynikających z Polityki.
2. Wszyscy Kwalifikowani dostawcy usług zaufania współpracujący z Pocztą Polską są zobowiązani spełniać wymagania bezpieczeństwa wynikające z Polityki.
3. Świadcząc Usługę RDE w oparciu o innych Dostawców usług zaufania, Poczta Polska zobowiązuje tych dostawców do spełnienia wymagań bezpieczeństwa wynikających z Polityki.

7.8.3. Zobowiązania Klientów

Klienci są zobowiązani do ochrony swoich danych dostępowych. Ponadto, Klienci ponoszą wyłączną odpowiedzialność za tworzenie lokalnych kopii zapasowych wysłanych i odebranych wiadomości.

7.9. Ograniczenia odpowiedzialności

1. Gwarancje Poczty Polskiej oparte są na ogólnych zasadach zawartych w Polityce oraz są zgodne z obowiązującymi aktualnie na terenie Rzeczypospolitej Polskiej nadrzędnymi aktami prawnymi.
2. Poczta Polska nie ponosi odpowiedzialności finansowej zdefiniowanej w Polityce wobec innych osób trzecich, niebędących odbiorcami Usług zaufania dostarczanych przez Pocztę Polską.
3. W celu nadzoru nad sprawnym działaniem Systemu RDE, rozliczania Klientów oraz Personelu pełniącego Role zaufane z ich działań, rejestrowane są wszystkie te zdarzenia występujące w systemie, które mają istotny wpływ na bezpieczeństwo funkcjonowania Systemu RDE.

7.10. Odszkodowania

Odszkodowanie z tytułu odpowiedzialności cywilnej wobec Klienta wynika ze zobowiązań i gwarancji określonych w treści Polityki.

7.11. Procedura wprowadzania zmian

1. Niezależnie od prowadzonych w Poczcie Polskiej audytów, raz w roku odbywa się przegląd obowiązującej wersji Polityki. Wyznaczone przez Zarząd Poczty Polskiej osoby analizują treść Polityki w kierunku jej zgodności z wdrożonymi procedurami oraz wymaganiami zewnętrznymi.
2. Zmiany treści Polityki mogą być wynikiem zauważonych błędów, uaktualnień oraz sugestii zainteresowanych Stron Usługi RDE.

3. Wszystkie wymienione w Polityce Strony Usługi RDE mają prawo wnieść propozycje zmian. Propozycje zmian mogą być nadsyłane pocztą tradycyjną lub elektroniczną na adresy kontaktowe Poczty Polskiej.
4. Jedynymi zmianami, które nie wymagają wcześniejszego informowania użytkowników, są zmiany wynikające z wprowadzenia korekt edycyjnych, zmiany w sposobie kontaktowania się z osobą odpowiedzialną za zarządzanie dokumentem, zmiany niemające rzeczywistego wpływu na znaczącą grupę użytkowników.
5. Po uprzednim poinformowaniu zainteresowanych Stron Usługi RDE, zmianom mogą podlegać dowolne elementy Polityki. Informacja o wszystkich istotnych, rozważanych zmianach w dokumencie jest przesyłana wszystkim zainteresowanym Stronom Usługi RDE w postaci informacji o miejscu dostępu nowej wersji Polityki.