Obowiązuje od 28 stycznia 2020 roku

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

Metryka dokumentu

Nazwa:	Polityka świadczenia usługi i deklaracja praktyk dla usługi rejestrowanego doręczenia elektronicznego w Poczcie Polskiej S.A.		
Identyfikator dokumentu	18/2020		
Wersja:	1.0	**Autor:**	Poczta Polska S.A.
Stron:	27	**Data:**	28.01.2020

1. Wstęp

1.1. Wprowadzenie

Niniejszy dokument: Polityka świadczenia usługi i deklaracja praktyki dla usługi rejestrowanego doręczenia elektronicznego w Poczcie Polskiej S.A. („**Polityka**"), określa ogólne zasady stosowane przez Pocztę Polską S.A. w trakcie świadczenia usługi zaufania - usługi rejestrowanego doręczenia elektronicznego, zarówno kwalifikowanej, jak i niekwalifikowanej.

Usługa jest świadczona zgodnie z:

1) Rozporządzeniem 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 („**Rozporządzenie eIDAS**");
2) ustawą z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej („**Ustawa**");
3) ustawą z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;
4) normami Europejskiego Instytutu Norm Telekomunikacyjnych („**ETSI**"):
   a) ETSI EN 319 401 v2.2.1 *Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers,*
   b) ETSI EN 319 521 V1.1.0 *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers.*
   c) Polityka definiuje Strony usługi, 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 -** oznaczają 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 lub niekwalifikowany dostawca usług zaufania;
3. **Dyrektor BIC** - Dyrektor Biura Inicjatyw Cyfrowych Poczty Polskiej S.A.;
4. **Krajowy Schemat Identyfikacji** - krajowy schemat identyfikacji elektronicznej obejmuje:
   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”);

5. **Kwalifikowany dostawca usług zaufania** – dostawca usług zaufania, któremu statusu kwalifikowany nadal organ nadzoru;
6. **Usługa RDE** – usługa rejestrowanego doręczenia elektronicznego umożliwiająca przesłanie danych między stronami trzecimi drogą elektroniczną i zapewniającą dowody związane z posługiwaniem się przesyłanymi danymi, w tym dowód wysłania i otrzymania danych, oraz chroniącą przesyłane dane przed ryzykiem utraty, kradzieży, uszkodzenia lub jakiejkolwiek nieupoważnionej zmiany; niekwalifikowana albo kwalifikowana spełniająca wymogi, o których mowa w art. 44 Rozporządzenia eIDAS;
7. **Personel –** osoby zatrudnione odpowiednio, przez PP lub PPUC, na podstawie umowy o pracę oraz osoby fizyczne świadczące osobiście usługi na rzecz PP lub PPUC w oparciu o umowę cywilnoprawną (umowę o dzieło, umowę zlecenia, umowę o świadczenie usług), w tym członkowie zarządu i rady nadzorczej;
8. **Poziom wiarygodności (bezpieczeństwa)** - poziomy bezpieczeństwa identyfikacji elektronicznej zgodnie z art. 8 rozporządzenia eIDAS; nazywane niekiedy jako poziomami zaufania lub wiarygodności, (tłum. z j. ang. *Level of assurance);*
9. **PP** - Poczta Polska S.A.;
10. **PPUC** – Poczta Polska Usługi Cyfrowe Sp. z o.o.;
11. **Przesyłka** – dane przesyłane pomiędzy stronami z wykorzystaniem usług RDE;
12. **Środek identyfikacji elektronicznej** – oznacza materialną lub niematerialną jednostkę zawierającą dane identyfikujące osobę i używaną do celów uwierzytelniania dla usługi online;
13. **Strony Usług RDE –** podmioty wskazane w podrozdziale 1.3 Polityki**;**
14. **System identyfikacji elektronicznej** - oznacza system identyfikacji elektronicznej, w ramach którego wydaje się środki identyfikacji elektronicznej osobom fizycznym lub prawnym, lub osobom fizycznym reprezentującym osoby prawne;
15. **System RDE** – oznacza wszystkie elementy organizacyjne i techniczne zapewniające funkcjonowanie Usługi RDE niekwalifikowanej albo kwalifikowanej;
16. **Role zaufane –** role pełnione przez wyznaczonych członków Personelu w zakresie wskazanym w podrozdziale 4.2.1 Polityki;
17. **Usługa zaufania** – świadczona za wynagrodzeniem usługa elektroniczna obejmująca czynności wskazane w art. 3 pkt 16 lit. a-c Rozporządzenia eIDAS**;**

1.3. Definicje Stron Usług RDE

Nazwa strony	Opis
Dostawca Usługi RDE	PP 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	Poczta Polska Usługi Cyfrowe Sp. z o.o. 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 niniejszym dokumencie
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 PP dostawca usługi zaufania, (np. kwalifikowanej usługi elektronicznego znacznika czasu lub usługi zaawansowanej pieczęci elektronicznej)

1.4. Zakres Usługi RDE

Zakresem objęta jest Usługa RDE zarówno niekwalifikowana, jak i kwalifikowana.

1) Dla wyżej wymienionych usług stosowana jest separacja w zakresie:
   a) baz danych,
   b) sprzętu kryptograficznego HSM, w tym kluczy kryptograficznych,
   c) uprawnień systemowych (istnieją różne systemy, sprzęt oraz stosowane klucze kryptograficzne).
2) Zarówno usługa kwalifikowana, jak i niekwalifikowana obsługiwane są przez wspólną infrastrukturę fizyczną (budynki) oraz infrastrukturę komunikacyjną (urządzenia sieciowe).

3) Ponadto dana usługa może korzystać, np. z danego rodzaju mechanizmu identyfikacji, natomiast wewnętrznie w ramach PP obsługa tego mechanizmu odbywa się w sposób odrębny dla usługi kwalifikowanej i niekwalifikowanej.
4) Usługa RDE może być realizowana przez jednego Dostawcę usług zaufania lub też umożliwiać doręczenie dzięki współpracy wielu Dostawców usług zaufania.
5) Wszyscy Kwalifikowani dostawcy usług zaufania współpracujący z PP 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, obejmuje 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, obejmuje następujące kroki:
      a) Dostawca Usługi RDE przekazuje do Klienta w roli odbiorcy informację, o gotowej do odbioru Przesyłce i prośbę, o akceptację przyjęcia Przesyłki;
      b) Klient może zaakceptować lub odmówić akceptacji Przesyłki, przy czym odmowa akceptacji Przesyłki może także zostać zrealizowana poprzez zaniechanie jej odbioru;
      c) Dostawca Usługi RDE wystawia dowód preawizacji Przesyłki;
      d) Usługa RDE identyfikuje i uwierzytelnia Klienta przed odbiorem Przesyłki;
      e) Następuje przekazanie Przesyłki poza usługę doręczenia – czyli do odbiorcy lub wskazanej przez niego skrzynki doręczeń.
   3) Wystawienie dowodów:
      a) Nadanie Przesyłki (w tym dokładny czas nadania) – dostępny dla nadawcy,
      b) Dowód preawizacji – dostępny dla nadawcy i odbiorcy,
      c) Odbiór 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 są zabezpieczone pieczęcią elektroniczną oraz znakowane czasem. PP udostępnia Klientom dowody wytworzone w procesie świadczenia Usługi RDE przez okres nie dłuższy niż 24 miesiące od momentu ich wytworzenia.

4. Niezależnie od utraty danych z powodów technicznych lub innych, PP 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. PP wskazuje Dyrektora BIC, jako podmiot odpowiedzialny za administrowanie Polityką.
2. Każdorazowa zmiana Polityki wymaga zatwierdzenia przez Zarząd PP. Z chwilą zatwierdzenia dokonanych zmian, w Metryce dokumentu wskazywany jest aktualny status danej wersji Polityki i data od której obowiązuje.
3. Za ocenę aktualności i przydatności Polityki odpowiada Dyrektor BIC.
4. W ramach świadczenia Usługi RDE, PP 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 dla Klientów oraz Stron ufających pod adresem www.poczta-polska.pl.
3. Wszelkie zmiany Polityki są aktualizowane, 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. PP w ramach Usługi RDE korzysta z zewnętrznego procesu identyfikacji elektronicznej, w ramach usługi nie jest wydawany środek uwierzytelniający.
2. Każdy adres doręczeń 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 umożliwia korzystanie ze wspólnej infrastruktury adresowej udostępnionej przez ministra właściwego ds. informatyzacji na podstawie właściwych przepisów.
3. Usługa RDE umożliwia mapowanie adresu doręczeń, 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 319411-1 i pr.;
   3) 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, gdy treść użytkownika zostanie wysłana lub przekazana. Jeżeli identyfikacja odbiorcy opiera się na zaawansowanym podpisie elektronicznym, weryfikacja podpisu poprzedza przekazanie treści użytkownika.
6. PP 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. PP posiada wewnętrzny dokument Polityki bezpieczeństwa informacji usługi rejestrowanego doręczenia elektronicznego w Poczcie Polskiej S.A. („Polityka bezpieczeństwa”), który określa podstawowe zasady zarządzania bezpieczeństwem informacji w zakresie Usługi RDE.
2. Polityka bezpieczeństwa jest komunikowana każdej osobie pełniącej Rolę zaufaną w zakresie Usługi RDE świadczonej przez PP, zaś PP jest zobowiązana do dokumentowania oświadczeń tych osób o zobowiązaniu się do przestrzegania zasad i wytycznych ujętych w Polityce.

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) oddalonych od siebie, wchodzących w skład infrastruktury krytycznej.

4.1.2. Dostęp fizyczny

1. Fizyczny dostęp do budynku oraz pomieszczeń wykorzystywanych w ramach świadczenia Usługi RDE jest kontrolowany oraz nadzorowany przez zintegrowany system zabezpieczenia teletechnicznego.
2. Ochrona na zewnątrz budynków funkcjonuje 24 godziny na dobę.
3. Pomieszczenia systemu komputerowego, w tym także pomieszczenia, w których znajduje się bezpieczny moduł kryptograficzny, wyposażone są w system kontroli dostępu do pomieszczeń oraz system sygnalizacji przeciwko włamaniom i napadom.
4. Dostęp do pomieszczeń wykorzystywanych w ramach świadczenia Usługi RDE posiadają tylko osoby upoważnione.
5. Nadzorowanie praw dostępu realizowane jest w oparciu o posiadane przez osoby upoważnione karty identyfikacyjne.

4.1.3. Bezpieczeństwo środowiskowe

1. W przypadku zaniku zasilania podstawowego System RDE przechodzi na zasilanie awaryjne poprzez UPS.
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 serwerowi 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 archiwa oraz bieżące kopie danych składowane są w sejfach ognioodpornych zlokalizowanych w centrum podstawowym. Dostęp do sejfów mają osoby pełniące rolę Inspektora bezpieczeństwa oraz Audytora.

4.1.5. Niszczenie informacji

Papierowe oraz elektroniczne nośniki zawierające informacje, mogące mieć wpływ na bezpieczeństwo PP, 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. 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 wykorzystywanym do świadczenia Usługi RDE pełnią określone Role zaufane, które zaprezentowano w poniższej tabeli. Przedstawiony podział ról został zatwierdzony uchwałą Zarządu PP i jest zgodny z wymogami: ETSI EN 319 401 Electronic Signatures and Infrastructures („ESI"); General Policy Requirements for Trust Service Providers.

Nazwa Roli zaufanej	Zakres głównych obowiązków
Dyrektor Biura Inicjatyw Cyfrowych	▪ Zapewnienie prawidłowej organizacji i funkcjonowania Usługi RDE. Wdrożenie/Wdrażanie postanowień Polityki. ▪ Określanie kierunków rozwoju Usługi RDE. ▪ Zapewnienie zgodności Usługi RDE z prawem oraz standardami normalizacyjnymi. ▪ Nadzorowanie zapewnienia ciągłości działania oraz zapewnienie realizacji planu zakończenia działalności.
Operator systemu	▪ Dbałość o operacyjne aspekty świadczenia Usługi RDE. ▪ Wykonywanie procedur i instrukcji operacyjnych. ▪ Realizacja procedur utrzymania Systemu RDE.
Administrator systemu	▪ Instalowanie, konfigurowanie i zarządzanie systemami oraz sieciami teleinformatycznymi wykorzystywanymi na potrzeby świadczenia Usługi RDE. ▪ 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 Polityki bezpieczeństwa, 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. ▪ Obsługa zgłoszeń zdarzeń i incydentów. ▪ 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 jednocześnie Usługi RDE oraz usług hybrydowych.

2. Wymienione w ust. 1 role i obowiązki związane z bezpieczeństwem (Inspektor bezpieczeństwa oraz Audytor) zostały również szczegółowo określone w dokumencie wewnętrznym jakim jest Polityka bezpieczeństwa.
3. PP 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 niego 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 wymienionych Ról zaufanych.

4.2.3. Zarządzanie incydentami

1. PP 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 zaufania.
2. PP bez zbędnej zwłoki, a w każdym razie nie później niż 24 godziny od otrzymania informacji o wystąpieniu zdarzenia, 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 PP 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 i uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) („RODO”) 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 PP procedurą zarządzania ryzykiem, w celu dostosowania zabezpieczeń techniczno-organizacyjnych do zidentyfikowanych zagrożeń dla aktywów Usługi RDE.

4.2.5. Nadzór nad Personelem pełniącym Role zaufane

4.2.5.1. Kwalifikacje, doświadczenie, upoważnienia

Osoby zajmujące się świadczeniem 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 Polityki bezpieczeństwa ,
4) nie wykonują obowiązków, które mogą doprowadzić do konfliktu interesów pomiędzy urzędem znakowania czasem, a działającymi w jego imieniu punktami rejestracji,
5) zapoznały się z wewnętrznymi procedurami PP 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 polityki, obowiązujących procedur oraz związanych z nimi zasad bezpieczeństwa.

4.2.5.2. Weryfikacja pracowników

1. Przed powierzeniem pracownikowi którejkolwiek z Ról zaufanych przeprowadzana jest co najmniej weryfikacja:
   1) świadectwa pracy z poprzedniego miejsca zatrudnienia (w przypadku nowego pracownika),
   2) dyplomu i świadectwa potwierdzających wykształcenie pracownika,
   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, przed dopuszczeniem do pełnienia swojej roli przeszły cykl szkoleń dotyczących:
   1) zasad określonych w Polityce,
   2) zasad zawartych w dokumentacji przypisanej roli, którą dana osoba pełni i zakresu obowiązków, które będą wykonywały,
   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 powyżej są powtarzane co najmniej raz do roku oraz w zależności od potrzeb zawsze wtedy, gdy nastąpiły istotne zmiany w świadczeniu Usługi RDE przez PP.

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 PP i może prowadzić do rozpoczęcia postępowania karnego.
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 PP 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

PP 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) wzorów umów oraz stosowanych formularzy wniosków,

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

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 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 rejestrowania przekazania 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 Polityką bezpieczeństwa, uruchamianiem i zamykaniem systemu, awariami systemu i awariami sprzętu, działaniami zapory i routera oraz próbami dostępu do Systemu RDE.
2. Ponadto PP 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, Dyrektor BIC oraz osoby upoważnione przez Dyrektora BIC.
5. Rejestry zdarzeń zapisywane są w formie elektronicznej. Rekordy zawierają: identyfikator zdarzenia, datę i czas wystąpienia, 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 dzienniku zdarzeń jest synchronizowany z UTC +01:00, co najmniej raz dziennie.

4.3.2. Tworzenie kopii zapasowych i odtwarzanie

1. Zapisy zdarzeń są kopiowane zgodnie z harmonogramem tworzenia kopii bezpieczeństwa systemu. 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 użytkowników,
   2) dane uwierzytelniające użytkowników,
   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 treści użytkownika,
   6) dowody na to, że treść użytkownika nie została zmodyfikowana podczas transmisji,
   7) odniesienie do lub przesłanie całej przesłanej treści użytkownika,
   8) tokeny znaczników czasu odpowiadające dacie i godzinie wysyłania, wysyłania i przekazywania oraz modyfikowania treści użytkownika, stosownie do przypadku,
   9) Politykę oraz jej historyczne wersje,
   10) inne dokumenty umieszczone w repozytorium zgodnie z zapisami Polityki.
2. Archiwum zawiera również wszelkie dokumenty papierowe, związane ze świadczeniem Usług zaufania, których okres przechowywania wynosi 20 lat zgodnie z art. 20 w zw. z art. 17 Ustawy.
3. PP zapewnia poufność, integralność i dostępność tworzonych dzienników.
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 PP

1. PP 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 Polityki, kontrahentów i partnerów z którymi PP jest związana umowami handlowymi, na których wykonanie zakończenie świadczenia usługi 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 PP określa Plan zakończenia działalności usługi rejestrowanego doręczenia elektronicznego w Poczcie Polskiej S.A..
3. Organ nadzoru jest informowany o planach zakończenia działalności w zakresie świadczenia Usługi RDE przez PP oraz każdorazowo o każdej jego zmianie.
4. PP 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 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 PP, 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 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. 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),
   2) uznaniową kontrolę dostępu,
   3) możliwość prowadzenia audytu zabezpieczeń,

4) komputery udostępniane są tylko osobom pełniącym Role zaufane,
5) pracownik, który pełni Role zaufaną, zobowiązany do blokowania swojej stacji roboczej zawsze, jeśli pozostają one poza jego nadzorem,
6) wymuszanie separacji obowiązków, wynikających z pełnionych zaufanych ról,
7) wymuszanie wylogowania użytkownika po okresie bezczynności,
8) identyfikację i uwierzytelnienie ról oraz pełniących je osób,
9) kryptograficzną ochronę sesji wymiany informacji oraz zabezpieczenia baz danych,
10) archiwizowanie historii czynności wykonywanych na komputerze oraz danych dla potrzeb audytu,
11) bezpieczną ścieżkę, pozwalającą na wiarygodną identyfikację i uwierzytelnienie ról oraz pełniących je osób,
12) mechanizm odtwarzania kluczy (tylko w przypadku modułów kryptograficznych) oraz systemu operacyjnego i aplikacji,
13) 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 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 PP 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 dowolne 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 specjaliści w roli Administratora 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,
   3) strefę chronioną stacji administratorów,
   4) strefę chronioną stacji audytorów,
   5) strefę ograniczonego zaufania z publicznymi serwerami usługowymi.
3. Dla wyżej wymienionych stref 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 oraz zabezpieczenie przed jakąkolwiek ingerencją w treść komunikacji.
6. W usłudze wykorzystywane są najnowocześniejsze protokoły i algorytmy do szyfrowania na poziomie warstwy transportowej. Usługi korzystają z certyfikatów uwierzytelniania strony 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.
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. PP 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 zewnętrznego dostępu do Usługi zaufania, zewnętrzne połączenia sieciowe będą nadmiarowe (redundantne) w celu zapewnienia dostępności usług, w przypadku pojedynczej awarii. Decyzje o podjęciu określonych środków bezpieczeństwa podejmowane są na mocy

prowadzonych analiz ryzyka, zgodnie z wewnętrzną procedurą. Usługa RDE łączy 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), PP 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 treści użytkownika 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. PP zapewnia sprawdzanie poprawności wygenerowanych pieczęci, jeżeli będzie korzystać z usługi zewnętrznego dostawcy usługi kwalifikowanej pieczęci.
4. PP 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 zarejestrowane Przesyłki (w tym dowody nadania i odbioru) przetwarzane przez Usługę zaufania są znakowane czasem, w oparciu o zewnętrznego kwalifikowanego dostawcę kwalifikowanego znacznika czasu (podstawowy dostawca usługi znakowania czasem).
2. PP 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 dostawcą usługi na wypadek niedostępności podstawowej usługi.

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, w tym klucze certyfikatów dla zaawansowanej pieczęci elektronicznych są przechowywane na kryptograficznych kartach inteligentnych. 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 PP 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, zgodnie z wewnętrzną Polityką audytu w zakresie usługi rejestrowanego doręczenia elektronicznego w Poczcie Polskiej S.A. lub
   2) 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 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 wydanymi decyzjami wykonawczymi do niego,
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 PP oraz Dyrektorowi BIC.
2. Zarząd powołuje zespół osób, w celu przygotowania w terminie określonym w raporcie, pisemnego stanowiska PP, 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 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: Zarząd PP, Dyrektor BIC, Inspektor Bezpieczeństwa.

7. Inne postanowienia

7.1. Opłaty

Z tytułu świadczonych usług zaufania PP pobiera opłaty według cennika publikowanego na stronie internetowej PP.

7.2. Niedyskryminujące zastosowanie

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

7.3. Odpowiedzialność finansowa

1. PP zapewnia, że zapewniono wystarczające środki finansowe na obsługę Usługi RDE i wypełnienie wszystkich zobowiązań dotyczących Usługi RDE.
2. Procedury mediacji i zwrotu roszczeń Klientów lub innych zaufanych stron są udokumentowane w innych wytycznych, zweryfikowanych przez organ oceny zgodności.
3. Wszystkie uzgodnienia, niezbędne do świadczenia usługi zaufania, z podwykonawcami, partnerami outsourcingowymi i stronami trzecimi, podlegają umowom i regulacjom obowiązującym w tym zakresie w PP.
4. PP 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. PP i osoby w niej zatrudnione, bądź podmioty dokonujące czynności operacyjno-technicznych, w ramach obsługi Systemu RDE są obowiązane do zachowania w tajemnicy, wszelkich informacji powziętych w trakcie zatrudnienia lub wykonywania czynności jak powyżej także po ustaniu okresu zatrudnienia bądź umocowania do ich wykonywania, w tym tajemnicy przedsiębiorstwa. Szczegółowy zakres tajemnicy przedsiębiorstwa określony jest w oddzielnych wewnętrznych zarządzeniach firmy. W szczególności dotyczy to:
   1) informacji wpływającej od/do użytkowników Usługi RDE,
   2) zapisów transakcji systemowych (zarówno w całości, jak też w postaci danych do przeglądu kontrolnego transakcji, tzw. rejestrów transakcji systemowych),
   3) raportów kontroli wewnętrznej oraz zewnętrznej,
   4) informacji o przedsięwziętych środkach zabezpieczających sprzęt oraz oprogramowanie, informacje o administrowaniu usługami zaufania oraz projektowanymi zasadami rejestrowania.

7.5. Ochrona danych osobowych

PP przetwarza dane osobowe (w szczególności dane użytkowników Usługi RDE) zgodnie z obowiązującymi w tym zakresie przepisami prawa oraz wewnętrzną dokumentacją ochrony danych osobowych. Informacje na ten temat są dostępne na stronie internetowej PP.

7.6. Prawo do własności intelektualnej

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

7.7. Zgodność z obowiązującym prawem

Funkcjonowanie PP 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 PP

1. PP 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 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 obejmujących 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+01:00, z dokładnością do 1 sekundy.

7.8.2. Zobowiązania zewnętrznych podmiotów

1. Celem realizacji Usług zaufania PP współpracuje z PPUC, która jest dostawcą technicznego rozwiązania, wykorzystywanego do świadczenia Usługi RDE oraz operatorem Systemu RDE. PPUC na podstawie umowy zawartej z PP zobowiązana jest do przestrzegania wymagań wynikających z Polityki.
2. Wszyscy Kwalifikowani dostawcy usług zaufania, współpracujący z PP są zobowiązani spełniać wymagania bezpieczeństwa wynikające z Polityki.

3. Świadcząc Usługę RDE w oparciu o innych Dostawców usług zaufania, PP zobowiązuje dostawców do spełnienia wymagań bezpieczeństwa wynikających z Polityki.

7.8.3. Zobowiązania klientów kwalifikowanej usługi rejestrowanego doręczenia elektronicznego

Klienci Usługi RDE 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 PP oparte są na ogólnych zasadach zawartych w Polityce oraz są zgodne z obowiązującymi aktualnie na terenie Rzeczypospolitej Polskiej nadrzędnymi aktami prawnymi.
2. PP nie ponosi odpowiedzialności finansowej zdefiniowanej w Polityce, wobec innych osób trzecich, niebędących odbiorcami Usług zaufania dostarczanych przez PP.
3. W celu nadzoru nad sprawnym działaniem Systemu RDE, rozliczania użytkowników 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 użytkownika wynika ze zobowiązań i gwarancji określonych w treści Polityki.

7.11.Procedura wprowadzania zmian

1. Niezależnie od prowadzonych w PP audytów, raz w roku odbywa się przegląd obowiązującej wersji Polityki. Wyznaczone przez Zarząd PP 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.
3. Wszystkie wymienione w Polityce Strony, mają prawo wnieść propozycje zmian. Propozycje zmian mogą być nadsyłane pocztą tradycyjną lub elektroniczną na adresy kontaktowe PP.
4. Jedynymi zmianami, które nie wymagają wcześniejszego informowania użytkowników są zmiany wynikające z wprowadzenia korekt edycyjnych, zmian w sposobie kontaktowania się z osobą odpowiedzialną za zarządzanie dokumentem, zmiany nie mające rzeczywistego wpływu na znaczącą grupę użytkowników. Takie zmiany nie podlegają procedurze zatwierdzania i zmienia się jedynie wersja Polityki.
5. Po uprzednim poinformowaniu zainteresowanych stron, zmianom mogą podlegać dowolne elementy Polityki. Informacja o wszystkich istotnych, rozważanych zmianach

w dokumencie jest przesyłana wszystkim zainteresowanym stronom w postaci informacji o miejscu dostępu nowej wersji Polityki.