Obowiązuje od 16 maja 2024 roku

Polityka świadczenia usługi i deklaracja praktyk

dla publicznej usługi rejestrowanego doręczenia elektronicznego w Poczcie Polskiej S.A.

Metryka dokumentu

Nazwa:	Polityka świadczenia usługi i deklaracja praktyk dla publicznej usługi rejestrowanego doręczenia elektronicznego w Poczcie Polskiej S.A.		
Identyfikator dokumentu	16/2024		
Wersja:	4.1	**Autor:**	Poczta Polska S.A.
Stron:	26	**Data:**	08.05.2024

1. Wstęp

1.1 Wprowadzenie

Niniejsza Polityka świadczenia usługi i deklaracja praktyk dla publicznej usługi rejestrowanego doręczenia elektronicznego w Poczcie Polskiej S.A. („Polityka") określa ogólne zasady stosowane przez Pocztę Polską S.A. w trakcie świadczenia publicznej usługi rejestrowanego doręczenia elektronicznego.

Polityka definiuje Strony publicznej usługi rejestrowanego doręczenia elektronicznego, określa ich obowiązki i odpowiedzialność oraz obszary zastosowań jej regulacji. Ponadto określa rozwiązania, w tym techniczne i organizacyjne, wskazujące warunki zabezpieczeń dla publicznej usługi rejestrowanego doręczenia elektronicznego.

1.2 Słownik

1. **Aplikacja kliencka** – systemy teleinformatyczne, których funkcjonowanie zapewniają: minister właściwy do spraw informatyzacji oraz minister właściwy do spraw gospodarki, umożliwiające dostęp użytkownikom do zasobów skrzynek doręczeń znajdujących się w systemie teleinformatycznym operatora wyznaczonego, umożliwiające dostęp użytkownikom do publicznej usługi rejestrowanego doręczenia elektronicznego oraz publicznej usługi hybrydowej, za pośrednictwem których przekazywane są do systemu operatora wyznaczonego dane o uwierzytelnieniu osoby fizycznej w sposób określony w art. 20a ust. 1 pkt 1 lub 2 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne z wykorzystaniem środka identyfikacji elektronicznej zapewniającego co najmniej średni poziom bezpieczeństwa, o którym mowa w art. 8 ust. 2 lit. b Rozporządzenia eIDAS oraz za pośrednictwem których przekazywane są do systemu operatora wyznaczonego inne dane niezbędne do świadczenia publicznej usługi rejestrowanego doręczenia elektronicznego oraz publicznej usługi hybrydowej;
2. **Dane identyfikujące osobę** – zestaw danych umożliwiających ustalenie tożsamości Klienta;
3. **Dostawca usług zaufania** – dostawca usługi zaufania (np. kwalifikowanej usługi rejestrowanego doręczenia elektronicznego, 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;
4. **Z-ca Dyrektora CTC ds. Cyfryzacji** – Zastępcaca Dyrektora Centrum Transformacji Cyfrowej ds. Cyfryzacji w Poczcie Polskiej S.A.;
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 art. 12 ust. 8 Rozporządzenia eIDAS („węzeł transgraniczny”);
7. **Kwalifikowany dostawca usług zaufania** – dostawca usług zaufania, któremu status kwalifikowany nadał organ nadzoru;
8. **Personel** – osoby zatrudnione przez Pocztę Polską na podstawie umowy o pracę oraz osoby fizyczne świadczące osobiście usługi na rzecz Poczty Polskiej w oparciu o umowę cywilnoprawną (umowę o dzieło, umowę zlecenia, umowę o świadczenie usług), w tym członkowie Zarządu i Rady Nadzorczej Poczty Polskiej;
9. **Poczta Polska** – Poczta Polska S.A.;
10. **Poziom wiarygodności (bezpieczeństwa)** – poziomy bezpieczeństwa identyfikacji elektronicznej zgodnie z art. 8 Rozporządzenia eIDAS, określane niekiedy jako poziomy zaufania lub wiarygodności (tłum. z j. ang. *Level of assurance);*
11. **Przesyłka** – dane przesyłane pomiędzy stronami z wykorzystaniem publicznej usługi rejestrowanego doręczenia elektronicznego ;
12. **PURDE** – publiczna usługa rejestrowanego doręczenia elektronicznego jako usługa rejestrowanego doręczenia elektronicznego, o której mowa w art. 3 pkt 36 Rozporządzenia eIDAS, świadczona przez Pocztę Polską;
13. **Regulamin** – Regulamin świadczenia publicznej usługi rejestrowanego doręczenia elektronicznego i publicznej usługi hybrydowej, dostępny na stronie internetowej www.bip.poczta-polska.pl/repozytorium/ oraz w każdej placówce Poczty Polskiej;
14. **Role zaufane** – role pełnione przez wyznaczonych członków Personelu w zakresie wskazanym w podrozdziale 4.2.1 Polityki;
15. **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;

16. **Skrzynka doręczeń** – narzędzie umożliwiające wysyłanie, odbieranie i przechowywanie danych zgodnie ze Standardem, w ramach publicznej usługi rejestrowanego doręczenia elektronicznego, a także w ramach publicznej usługi hybrydowej;
17. **Standard** – standard publicznej usługi rejestrowanego doręczenia elektronicznego, świadczonej przez operatora wyznaczonego i kwalifikowanych dostawców usług zaufania świadczących kwalifikowane usługi rejestrowanego doręczenia elektronicznego w zakresie współpracy z publiczną usługą rejestrowanego doręczenia elektronicznego oraz skrzynki doręczeń, o którym mowa w art. 26a ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej, w wersji 1.1;
18. **Strony PURDE** – podmioty wskazane w podrozdziale 1.3 Polityki;
19. **System identyfikacji elektronicznej** – system, w ramach którego wydaje się środki identyfikacji elektronicznej Klientom;
20. **System OW** – elementy organizacyjne i techniczne zapewniające funkcjonowanie PURDE i PUH, którego częścią są skrzynki doręczeń;
21. **Środek identyfikacji elektronicznej** – materialna lub niematerialna jednostka zawierająca dane identyfikujące osobę i używana do celów uwierzytelniania dla usługi online;
22. **UoDE** – ustawa z dnia 18 listopada 2020 r. o doręczeniach elektronicznych;
23. **Usługa zaufania** – świadczona za wynagrodzeniem usługa elektroniczna obejmująca czynności wskazane w art. 3 pkt 16 lit. a-c Rozporządzenia eIDAS;
24. **Ustawa** – ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej.

1.3 Definicje Stron PURDE

Nazwa strony	Opis
Dostawca PURDE	Poczta Polska będąca dostawcą PURDE
Dostawca usługi RDE	Dostawca usługi rejestrowanego doręczenia elektronicznego, inny niż dostawca PURDE
Dostawca usługi identyfikacji elektronicznej	Dostawca środka identyfikacji elektronicznej w ramach notyfikowanego Krajowego Schematu Identyfikacji elektronicznej, zapewniający klientom usługi możliwość identyfikacji i uwierzytelnienia
Klient	Podmiot publiczny, podmiot niepubliczny (w tym osoba fizyczna), będący nadawcą lub odbiorcą PURDE

Strona ufająca	Klient polegający na zaufaniu do PURDE

1.4 Podstawowe elementy PURDE

1. PURDE składa się z następujących elementów: nadania Przesyłki, doręczenia Przesyłki i wystawienia dowodów dokonanych czynności:
   1) nadanie Przesyłki, obejmujące następujące kroki:
      a) identyfikację i uwierzytelnienie Klienta realizującego nadanie Przesyłki w Systemie OW,
      b) przekazanie przez Klienta Przesyłki do nadania przez Dostawcę PURDE,
      c) wystawienie dowodu wysłania przez Dostawcę PURDE,
   2) doręczenie Przesyłki, obejmujące następujące kroki:
      a) w przypadku adresata obsługiwanego przez Dostawcę PURDE:
         - przekazanie do Klienta w roli odbiorcy w Systemie OW informacji o gotowej do odbioru Przesyłce,
         - wystawienie przez Dostawcę PURDE dowodu preawizacji Przesyłki,
         - identyfikację i uwierzytelnienie Klienta umożliwiające odbiór Przesyłki,
         - wystawienie dowodu otrzymania przez Dostawcę PURDE,
      b) w przypadku adresata obsługiwanego przez Dostawcę usługi RDE - przekazanie przesyłki do Dostawcy usługi RDE,
   3) wystawienie dowodów:
      a) wysłania Przesyłki – dostępny dla Klienta będącego nadawcą PURDE,
      b) przekazania Przesyłki pomiędzy Dostawcą usług RDE a Dostawcą PURDE, z obowiązkiem przekazania dowodu wysłania,
      c) preawizacji (dowód przygotowania Przesyłki do odbioru/dowód o wysłaniu notyfikacji o Przesyłce gotowej do odbioru) – dostępny dla Klienta będącego nadawcą i Klienta będącego odbiorcą,
      d) otrzymania Przesyłki – dostępny dla Klienta będącego nadawcą i Klienta będącego odbiorcą (generowany także w przypadku zaniechania odbioru).
2. Przesyłka przekazywana do Dostawcy PURDE nie będzie przyjęta przez Dostawcę PURDE w przypadku, gdy:
   1) do przesyłki nie zostanie dołączony dowód wysłania, lub
   2) przesyłka będzie zaadresowana do więcej niż jednego adresata.
3. Każda zmiana danych niezbędna do celów wysłania lub otrzymania danych jest wyraźnie wskazana Klientowi będącemu nadawcą (przed nadaniem) i Klientowi będącemu odbiorcą (przed odbiorem) danych w postaci komunikatu elektronicznego.

4. Informacje o przesyłce w wystawianych przez Dostawcę PURDE dowodach są tworzone z wykorzystaniem funkcji skrótu SHA3-512.
5. Przekazywane do Dostawcy PURDE, wystawione przez Dostawcę usługi RDE, dowody zawierające informacje o przesyłce, wykorzystujące funkcję skrótu inną niż SHA3-512, nie będą przyjmowane przez Dostawcę PURDE.
6. Dowody w zakresie nadania, preawizacji oraz doręczenia są zabezpieczone pieczęcią elektroniczną oraz znakowane czasem. Poczta Polska udostępnia Klientom dowody wytworzone w procesie świadczenia PURDE przez okres nie dłuższy niż 36 miesięcy od momentu ich wytworzenia.
7. 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 PURDE, 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,
   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.
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 PURDE korzysta z zewnętrznego procesu identyfikacji elektronicznej, w ramach PURDE nie jest wydawany środek uwierzytelniający.
2. Każdy adres do doręczeń elektronicznych zapewnia jednoznaczną identyfikację nadawcy oraz odbiorcy. W zakresie adresacji usługa umożliwia korzystanie ze wspólnej infrastruktury adresowej udostępnionej przez ministra właściwego do spraw informatyzacji na podstawie właściwych przepisów.
3. PURDE umożliwia mapowanie adresu doręczeń, w szczególności w zakresie akceptacji wiadomości pochodzących od innych Dostawców usługi RDE, a także wiadomości doręczanych w ramach krajowego systemu e-doręczeń.
4. W ramach PURDE Dostawca PURDE dokonuje weryfikacji tożsamości nadawcy i adresata albo Dostawcy usługi RDE, nadawcy i adresata bezpośrednio lub polegając na stronie trzeciej. Dopuszcza się następujące sposoby identyfikacji i uwierzytelnienia:
   1) za pomocą certyfikatu zaawansowanego podpisu elektronicznego lub zaawansowanej pieczęci elektronicznej, lub
   2) stosując metody identyfikacji uznane na poziomie krajowym, które zapewniają równoważną pewność pod względem wiarygodności fizycznej obecności, lub
   3) wzajemne uwierzytelnianie z wykorzystaniem bezpiecznego protokołu oraz certyfikatów uznawanych w ramach PURDE, lub
   4) środek uwierzytelniający o równoważnym poziomie bezpieczeństwa ze wskazanymi powyżej.
5. Identyfikacja elektroniczna przeprowadzana jest za każdym razem przed nadaniem lub doręczeniem Przesyłki.
6. Poczta Polska, wykorzystując do identyfikacji elektronicznej zewnętrzne systemy identyfikacji elektronicznej zapewnia, że systemy te są uznane krajowo oraz oferują identyfikację bezpieczeństwa na co najmniej średnim poziomie wiarygodności.

4. Zabezpieczenia organizacyjne, operacyjne i fizyczne

1. Poczta Polska posiada wewnętrzny dokument dotyczący polityki bezpieczeństwa informacji, który określa nadrzędne zasady zarządzania bezpieczeństwem informacji w zakresie PURDE.
2. Wewnętrzny dokument dotyczący polityki bezpieczeństwa informacji jest komunikowany każdej osobie pełniącej Rolę zaufaną w zakresie PURDE 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 PURDE mieszczą się w dwóch niezależnych i oddalonych od siebie lokalizacjach (centrum podstawowym i centrum zapasowym).

4.1.2 Dostęp fizyczny

1. Fizyczny dostęp do budynku oraz pomieszczeń wykorzystywanych w ramach świadczenia PURDE jest kontrolowany przez pracowników ochrony oraz nadzorowany przez elektroniczny system zabezpieczenia technicznego.
2. Ochrona fizyczna budynków funkcjonuje 24 godziny na dobę.
3. Pomieszczenia wykorzystywane w ramach świadczenia PURDE, w tym także pomieszczenia, w których znajduje się sprzętowy moduł bezpieczeństwa, wyposażone są w elektroniczny system kontroli dostępu do pomieszczeń oraz system sygnalizacji włamania i napadu. Dostęp do pomieszczeń wykorzystywanych w ramach świadczenia PURDE posiadają tylko osoby upoważnione.
4. 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 komponenty techniczne Systemu OW przechodzą na zasilanie awaryjne.
2. Środowisko pracy w pomieszczeniach wykorzystywanych w ramach świadczenia PURDE 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 wykorzystywanych w ramach świadczenia PURDE, 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 archiwa oraz bieżące kopie danych, składowane są w bezpiecznych lokalizacjach. Dostęp do nich mają osoby pełniące Role zaufane.

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 OW 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 PURDE. Wdrożenie/Wdrażanie postanowień Polityki. ▪ Zapewnienie zgodności PURDE 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 OW. ▪ Realizacja kierunków rozwoju usług. ▪ Utrzymanie aktualności planu zakończenia działalności.
Operator systemu	▪ Dbałość o operacyjne aspekty świadczenia PURDE. ▪ Wykonywanie procedur i instrukcji operacyjnych. ▪ Realizacja procedur utrzymania Systemu OW.
Administrator systemu	▪ Nadzór nad instalowaniem, konfigurowaniem i zarządzaniem systemami oraz sieciami teleinformatycznymi wykorzystywanymi na potrzeby świadczenia PURDE. ▪ Operacyjne czynności w zakresie zarządzania kluczami.
Inspektor bezpieczeństwa	▪ Zapewnienie bezpieczeństwa procesu w ramach świadczonej PURDE. ▪ 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 PURDE.

Audytor	▪ Przeglądanie archiwów i rejestrów zdarzeń PURDE. ▪ Analizowanie zdarzeń i incydentów dotyczących PURDE. ▪ Rekomendowanie działań naprawczych i profilaktycznych. ▪ Kontrola wdrożonych mechanizmów i środków bezpieczeństwa.
Koordynator ds. wdrożenia eUsług	▪ Koordynowanie działań dotyczących jednocześnie PURDE oraz usług hybrydowych.
Inspektor ds. weryfikacji 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 OW.

4.2.2 Role zaufane podlegające separacji obowiązków

1. Role zaufane wyodrębnione w ramach Personelu zapobiegają nadużyciom, przy korzystaniu z Systemu OW.
2. Każdej osobie odpowiedzialnej za eksploatację Systemu OW 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 wymienionych Ról zaufanych.

4.2.3 Zarządzanie incydentami

1. Poczta Polska na żądanie ministra właściwego do spraw 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. Poczta Polska bez zbędnej zwłoki, nie później niż 24 godziny od otrzymania informacji o wystąpieniu incydentu, zawiadamia ministra właściwego do spraw informatyzacji, a w stosownych przypadkach, również 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 PURDE 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 Systemu OW.

4.2.5 Nadzór nad Personelem pełniącym Role zaufane

4.2.5.1 Kwalifikacje, doświadczenie, upoważnienia

1. Osoby pełniące Role zaufane posiadają odpowiednie kwalifikacje, 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 PURDE 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 PURDE,
   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.
2. Dopuszcza się zatrudnienie osób pełniących Role zaufane na umowę o pracę oraz na umowy cywilnoprawne (umowę o dzieło, umowę zlecenie, umowę o świadczenie usług).
3. Zakres odpowiedzialności osób fizycznych świadczących usługi na rzecz Poczty Polskiej w oparciu o umowy cywilnoprawne został zdefiniowany w stosownych umowach dotyczących współpracy.

4.2.5.2 Weryfikacja Personelu

1. Przed powierzeniem Personelowi którejkolwiek z Ról zaufanych przeprowadzana jest co najmniej weryfikacja:

1) świadectwa pracy z poprzedniego miejsca 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, przed dopuszczeniem do pełnienia swojej roli, przeszły 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 PURDE,
   6) oprogramowania systemu komputerowego PURDE,
   7) procedur realizowanych po awariach Systemu OW lub katastrofach wpływających na System OW,
   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 PURDE 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 OW 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 Dokumentacja dla Personelu pełniącego Role zaufane

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

1) Polityki,
2) Regulaminu,

3) procedur eksploatacyjnych w zakresie obsługi Systemu OW,
4) stosowanych formularzy wniosków,
5) niezbędnych wyciągów z dokumentacji (właściwej dla pełnionej Roli zaufanej), w tym procedur awaryjnych,
6) zakresu obowiązków i uprawnień wynikających z pełnionej Roli zaufanej.

4.3 Bezpieczna eksploatacja

4.3.1 Rejestrowanie zdarzeń

1. W ramach PURDE 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 uwierzytelnieniem Klientów PURDE,
      d) czynności związane z uwierzytelnieniem dostawców usług RDE,
      e) czynności związane z obsługą Klientów, w tym dowody w zakresie rejestrowania nadania i doręczania Przesyłek,
   2) logi systemowe z serwerów i stacji roboczych wchodzących w skład Systemu OW,
   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 OW, awariami Systemu OW i awariami sprzętu, działaniami zapory i routera oraz próbami dostępu do Systemu OW.
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

Tworzenie kopii zapasowych i ich odtwarzanie jest wykonywane zgodnie z wewnętrzną polityką kopii bezpieczeństwa dla Systemu OW.

4.3.3 Archiwizacja zdarzeń

1. W ramach PURDE archiwizacji podlegają w szczególności:
    1) dane uwierzytelniające Klienta,
    2) logi operacji w zakresie PURDE, weryfikacji tożsamości Klienta będącego nadawcą i Klienta będącego odbiorcą oraz dostawcy usługi RDE,
    3) dowody na to, że treść Przesyłki nie została zmodyfikowana podczas transmisji,
    4) tokeny znaczników czasu odpowiadające dacie i godzinie wysyłania i przekazywania oraz modyfikowania treści Przesyłki, stosownie do przypadku,
    5) Polityka oraz jej historyczne wersje,
    6) 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. 17 z zastrzeżeniem art. 20 ust. 1 Ustawy.
3. Poczta Polska zapewnia poufność, integralność i dostępność tworzonych rejestrów zdarzeń.
4. Zapisy dotyczące funkcjonowania PURDE są udostępniane, jeśli jest to wymagane, w celu udokumentowania prawidłowego działania PURDE dla celów postępowania sądowego.

4.3.4 Zakończenie działalności w zakresie PURDE lub przekazanie zadań przez Pocztę Polską

1. Poczta Polska, mając na uwadze redukcję wpływu skutków podjęcia potencjalnej decyzji o zakończeniu świadczenia działalności w zakresie PURDE, planuje w szczególności spełnienie obowiązku odpowiednio wczesnego poinformowania o tym organu nadzoru, wszystkich Stron PURDE, kontrahentów i partnerów, z którymi Poczta Polska jest związana umowami, na których wykonanie zakończenie świadczenia PURDE 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 PURDE przez Pocztę Polską określa Plan zakończenia działalności w ramach publicznej usługi rejestrowanego doręczenia elektronicznego w Poczcie Polskiej S.A.
3. Organ nadzoru jest informowany o planach zakończenia działalności w zakresie świadczenia PURDE przez Pocztę Polską oraz każdorazowo o każdej jego zmianie.
4. Poczta Polska zobowiązuje się do wykonania następujących czynności:

1) zapewnienia ciągłości pełnienia roli dostawcy PURDE nie dłużej niż 3 miesiące od dnia poinformowania organu nadzoru, o zamiarze zaprzestania bądź niemożności pełnienia roli podmiotu dostawcy PURDE,
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 PURDE w imieniu Poczty Polskiej, nie później niż na dzień zakończenia działalności w zakresie świadczenia PURDE,
4) przekazania do zniszczenia lub wycofania kluczy prywatnych, w tym kopii zapasowych, w taki sposób, aby klucze prywatne nie mogły zostać odzyskane.

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 PURDE.
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 OW.
2. Funkcje zabezpieczające systemów komputerowych są realizowane na poziomie systemu operacyjnego, aplikacji oraz zabezpieczeń fizycznych.
3. Personel, który pełni Rolę zaufaną, zobowiązany jest do blokowania swoich stacji roboczych zawsze, jeśli pozostają one poza jego nadzorem.
4. Komputery pracujące w Systemie OW wyposażone są w następujące funkcje zabezpieczające:
   1) obligatoryjnie uwierzytelnione rejestrowanie się na poziomie systemu operacyjnego i aplikacji,
   2) uznaniową kontrolę dostępu,
   3) możliwość prowadzenia audytu zabezpieczeń,
   4) udostępnianie tylko Personelowi pełniącemu Role zaufane,
   5) wymuszanie separacji obowiązków wynikających z pełnionych Ról zaufanych,
   6) wymuszanie wylogowania osoby pełniącej Rolę zaufaną po okresie bezczynności,
   7) identyfikację i uwierzytelnienie Ról zaufanych oraz pełniących je osób,
   8) kryptograficzną ochronę sesji wymiany informacji oraz zabezpieczenia baz danych,

9) archiwizowanie historii czynności wykonywanych na komputerze oraz danych dla potrzeb audytu,
10) bezpieczny kanał pozwalający 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 OW sprawuje Inspektor bezpieczeństwa. Zatwierdza on konfigurację Systemu OW 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 OW, integralność jego zasobów oraz zachowanie poufności danych.
3. Kontrola zarządzania bezpieczeństwem ma na celu takie nadzorowanie funkcjonowania Systemu OW, 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 OW są rejestrowane, to każda z wprowadzonych zmian wymaga dodatkowo zweryfikowania i akceptacji przez przynajmniej dwie osoby pełniące Role zaufane: Inspektora bezpieczeństwa oraz Administratora systemu.
5. System kontroli zmiany informuje uprawnionych pracowników o wystąpieniu modyfikacji w Systemie OW i wymaga jej weryfikacji przez osobę inną od tej, która wprowadzała daną zmianę.
6. Aktualna konfiguracja Systemu OW, jak również modyfikacje i aktualizacje tego systemu są dokumentowane i kontrolowane. Zastosowane w Systemie OW 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 OW sprawują specjaliści w roli Administratora systemu.

2. Sieć w ramach Systemu OW 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 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 w Systemie OW jest realizowana za pomocą szyfrowanych kanałów, zabezpieczających przed ingerencją w treść komunikacji.
6. W usłudze wykorzystywane są najnowocześniejsze protokoły i algorytmy do szyfrowania na poziomie warstwy transportowej. Usługi korzystają z certyfikatów uwierzytelniania stron, 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 OW 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 dostępu do PURDE, zewnętrzne połączenia sieciowe będą nadmiarowe (redundantne) w celu zapewnienia dostępności usługi, w przypadku pojedynczej awarii. Decyzje o podjęciu określonych środków bezpieczeństwa podejmowane są na mocy prowadzonych analiz ryzyka, zgodnie z wewnętrzną procedurą. PURDE, łącząc się z innymi Dostawcami usług zaufania 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

i Operatora systemu. W przypadku znaczących zmian w konfiguracji Systemu OW, Poczta Polska zapewnia przeprowadzenie testów bezpieczeństwa oraz gromadzi dowody z prowadzonych testów.

5.4 Zabezpieczenie Przesyłek

1. Wszystkie Przesyłki są zabezpieczone za pomocą zaawansowanych mechanizmów kryptograficznych. Integralność treści Przesyłki i związanych z nią metadanych jest chroniona podczas transmisji, w szczególności w przypadku wymiany z nadawcą/odbiorcą/Dostawcą usługi RDE lub między rozproszonymi komponentami Systemu OW, a także w pamięci masowej. Ochrona integralności jest realizowana poprzez zastosowanie mechanizmów kryptograficznych, np. pieczęci elektronicznych.
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 zarejestrowane Przesyłki (w tym dowody wysłania i otrzymania) przetwarzane przez Usługę zaufania są znakowane czasem, w oparciu o zewnętrznego kwalifikowanego dostawcę kwalifikowanego znacznika czasu (podstawowy dostawca usługi znakowania czasem).
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 Dostawcą usługi zaufania na wypadek niedostępności usługi u podstawowego dostawcy usługi znakowania czasem.
4. Lista kwalifikowanych dostawców, z którymi współpracuje Poczta Polska w zakresie świadczenia PURDE, udostępniona jest na stronie internetowej www.edoreczenia.poczta-polska.pl.

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 elektronicznej 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 PURDE 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

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

6.1. Częstotliwość i okoliczności oceny

1. Audyt przeprowadzany jest samodzielnie przez Audytorów, zgodnie z wewnętrzną polityką audytu dotyczącą Systemu OW.
2. Audyt zewnętrzny może być przeprowadzony w trybie wskazanym w UoDE.

6.2. Zagadnienia objęte audytem

Do zagadnień objętych audytem należy w szczególności sprawdzenie wymagań:

1) organizacyjno-prawnych wynikających z UoDE oraz rozporządzeń wykonawczych do UoDE,
2) wynikających ze Standardu.

6.3. Działania podejmowane celem usunięcia usterek wykrytych podczas audytu

1. Raporty audytów 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 do spraw 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.

6.4. 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

Dostawca PURDE pobiera opłatę za świadczenie PURDE zgodnie z cennikiem usług opublikowanym na stronie internetowej Poczty Polskiej www.bip.poczta-polska.pl/repozytorium/.

7.2. Odpowiedzialność finansowa

1. Poczta Polska potwierdza, że zapewniono wystarczające środki finansowe na obsługę PURDE i wypełnienie wszystkich zobowiązań dotyczących PURDE.
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.

7.3. Poufność informacji

Personel zatrudniony w Poczcie Polskiej bądź podmioty dokonujące czynności operacyjno-technicznych w ramach obsługi Systemu OW 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 odrębnych wewnętrznych aktach prawnych Poczty Polskiej. W szczególności dotyczy to:

1) informacji wpływającej od/do Klientów PURDE oraz Dostawców usług 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.

7.4. Ochrona danych osobowych

Poczta Polska przetwarza dane osobowe (w szczególności dane Klientów) zgodnie z obowiązującymi w tym zakresie przepisami prawa oraz wewnętrzną dokumentacją ochrony danych osobowych. Informacje na ten temat są dostępne w Regulaminie i na stronie internetowej Poczty Polskiej.

7.5. 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.

7.6. Zgodność z obowiązującym prawem

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

7.7. Zobowiązania i gwarancje

7.7.1. Zobowiązania Poczty Polskiej

1. Poczta Polska gwarantuje, że postępuje zgodnie z prawem, a w szczególności:
   1) nie narusza postanowień UoDE wraz z przepisami wykonawczymi,
   2) nie narusza postanowień Standardu,
   3) nie narusza postanowień Rozporządzenia eIDAS, Ustawy wraz z przepisami wykonawczymi oraz nie narusza praw autorskich i licencyjnych stron trzecich,
   4) 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 PURDE są synchronizowane z międzynarodowym wzorcem czasu UTC, z dokładnością do 1 sekundy.

7.7.2. Zobowiązania zewnętrznych podmiotów

1. Celem realizacji PURDE Poczta Polska współpracuje z ministrem właściwym do spraw informatyzacji oraz ministrem właściwym do spraw gospodarki, którzy są dostawcą Aplikacji klienckiej, wykorzystywanej do świadczenia PURDE.
2. Wszyscy Dostawcy usług zaufania, współpracujący z Pocztą Polską, są zobowiązani spełniać wymagania bezpieczeństwa wynikające z Polityki.
3. Świadcząc PURDE w oparciu o innych Dostawców usług zaufania, Poczta Polska zobowiązuje dostawców do spełnienia wymagań bezpieczeństwa wynikających z Polityki.

7.7.3. Zobowiązania klientów PURDE

Klienci PURDE są zobowiązani do ochrony swoich danych dostępowych. Ponadto, Klienci ponoszą wyłączną odpowiedzialność za tworzenie lokalnych kopii zapasowych nadanych i doręczonych Przesyłek.

7.8. Ograniczenia odpowiedzialności

1. Odpowiedzialność Poczty Polskiej oparta jest na ogólnych zasadach zawartych w Polityce i Regulaminie oraz jest zgodna z UoDE oraz 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 OW, 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 OW.
4. W przypadku wymiany danych pomiędzy Dostawcą PURDE a Dostawcą usługi RDE:
   1) odpowiedzialność Poczty Polskiej w przypadku PURDE, której nadawca korzysta z usług Dostawcy usługi RDE, rozpoczyna się od momentu przyjęcia przesyłki do Systemu OW adresata, czyli od momentu potwierdzenia przyjęcia przesyłki przez System OW poprzez komunikat „SignalMessage typu Receipt”,
   2) odpowiedzialność Poczty Polskiej w przypadku PURDE, której adresat korzysta z usług Dostawcy usługi RDE, kończy się w momencie przekazania przesyłki do Dostawcy usługi RDE adresata, czyli od momentu potwierdzenia przyjęcia przesyłki przez system Dostawcy usługi RDE poprzez komunikat „SignalMessage typu Receipt”,
   3) Dostawca usługi RDE jest zobowiązany do przekazania do Systemu OW dowodu D.1, w przypadku otrzymania z Systemu OW przesyłki do doręczenia na rzecz adresata, korzystającego z usług Dostawcy usługi RDE. Poczta Polska nie ponosi odpowiedzialności z tytułu niedoręczenia potwierdzenia otrzymania w przypadku, gdy Dostawca usługi RDE adresata nie przekaże do Systemu OW właściwego dowodu D.1,
   4) czas na doręczenie przesyłki w przypadku PURDE liczony jest przez Pocztę Polską:
      a) od momentu nadania przesyłki PURDE w Poczcie Polskiej do momentu przekazania jej do systemu Dostawcy usługi RDE,
      b) od momentu przyjęcia przesyłki do doręczenia z systemu Dostawcy usługi RDE do jej doręczenia adresatowi za pośrednictwem Systemu OW.

7.9. Odszkodowanie

Odszkodowanie z tytułu odpowiedzialności wobec Klienta wynika z zobowiązań określonych w treści Polityki, Regulaminu i obowiązujących przepisów prawa.

7.10. 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.
3. Wszystkie wymienione w Polityce strony 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 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.

7.11. Zasady wykorzystywane w protokole AS4 przez Pocztę Polską

1. W celu wymiany danych z Systemem OW w zakresie funkcjonowania z PURDE konieczne jest przeprowadzenie integracji systemu Dostawcy usługi RDE z Systemem OW.
2. Warunki integracji, o której mowa w ust. 1, dostępne są na stronie internetowej www.edoreczenia.poczta-polska.pl i obowiązują od momentu opublikowania ich na tej stronie.
3. Zasady integracji, o której mowa w ust. 1, są zgodne ze Standardem.
4. Warunkiem koniecznym do uruchomienia komunikacji w protokole AS4 pomiędzy Dostawcą usługi RDE a Systemem OW jest zakończenie z wynikiem pozytywnym testów integracyjnych przeprowadzonych przez Dostawcę usługi RDE na środowisku testowym krajowego systemu e-doręczeń, o którym mowa w Standardzie.