Doręczenia elektroniczne

Zbiór dokumentów opisujących wykonywanie przez KFJ Inwestycję sp. z o.o. usługi Rejestrowanego Doręczenia Elektronicznego [RDE] będącej usługą zaufania

---

Grupa 01 Dokumenty podstawowe

01.02 Polityka świadczenia przez KFJ Inwestycje usługi KURDE

Grupa 01	**Dokumenty podstawowe**		
Tytuł dokumentu	Polityka świadczenia przez KFJ Inwestycje usługi KURDE		
Identyfikator dokumentu	01.02	**Klasyfikacja informacji**	Publiczny
Wersja	3.2	**Autor**	Filip Lemka
Data opracowania	09.04.2022	**Zatwierdził**	Zarząd KFJ

Historia zmian

Wersja	Autor	Zatwierdził	Data	Komentarz
1.0	G.Lemka	Zarząd KFJ	2019.12.15	Pierwsza wersja dokumentu
2.0	F.Lemka	Zarząd KFJ	2021.04.12	Generalna zmiana dokumentu
3.0	F.Lemka	Zarząd KFJ	2022.02.20	Generalna zmiana dokumentu
3.1	F.Lemka	Zarząd KFJ	2022.02.26	Zmieniono pkt. 1 Dodano w sekcji 1.4 pkt. 6, 7 i 8 Dodano pkt. 3 i 4 w sekcji 7.6.2 Dodano: sekcję 8
3.2	F.Lemka	Zarząd KFJ	2022.04.09	Zmieniono pkt. 8.2

Spis Treści

1.Wstęp

1.1.Wprowadzenie

Niniejsza Polityka świadczenia usługi i deklaracja praktyki dla kwalifikowanej usługi rejestrowanego doręczenia elektronicznego w KFJ Inwestycje Sp. z o.o. („Polityka") określa ogólne zasady stosowane przez KFJ Inwestycje Sp. z o.o. w trakcie świadczenia kwalifikowanej usługi rejestrowanego doręczenia elektronicznego zgodnej z 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.

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

1.2.Słownik

1) **Dane identyfikujące osobę** - zestaw danych umożliwiających ustalenie tożsamości Klienta;
2) **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;
3) **Dyrektor KFJ** - Dyrektor KFJ Inwestycje Sp. z o.o.;
4) **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;
5) **KFJ** - KFJ Inwestycje Sp. z o.o.;

6) **KURDE** – kwalifikowana usługa rejestrowanego doręczenia elektronicznego jako usługa rejestrowanego doręczenia elektronicznego, o której mowa w art. 3 pkt 37 Rozporządzenia eIDAS, świadczona przez KFJ;
7) **Kwalifikowany dostawca usług zaufania** – dostawca usług zaufania, któremu status kwalifikowany nadał organ nadzoru;
8) **Personel** – osoby zatrudnione przez KFJ na podstawie umowy o pracę oraz osoby fizyczne świadczące osobiście usługi na rzecz KFJ w oparciu o umowę cywilnoprawną (umowę o dzieło, umowę zlecenia, umowę o świadczenie usług);
9) **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);
10) **Przesyłka** – dane przesyłane pomiędzy stronami z wykorzystaniem KURDE;
11) **Regulamin** – Regulamin świadczenia kwalifikowanej usługi rejestrowanego doręczenia elektronicznego KFJ Inwestycje Sp. z o.o., dostępny na stronie internetowej doreczeniaelektroniczne.pl;
12) **Role zaufane** – role pełnione przez wyznaczonych członków Personelu w zakresie wskazanym w podrozdziale 4.2.1 Polityki;
13) **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;
14) **Skrzynka doręczeń** – narzędzie umożliwiające wysyłanie, odbieranie i przechowywanie danych zgodnie ze Standardem, w ramach kwalifikowanej usługi rejestrowanego doręczenia elektronicznego;
15) **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;
16) **Strony KURDE** – podmioty wskazane w podrozdziale 1.3 Polityki;
17) **System identyfikacji elektronicznej** – system, w ramach którego wydaje się środki
identyfikacji elektronicznej Klientom;
18) **System KURDE** – elementy organizacyjne i techniczne zapewniające funkcjonowanie KURDE, którego częścią są skrzynki doręczeń;

19) **Środek identyfikacji elektronicznej** – materialna lub niematerialna jednostka zawierająca dane identyfikujące osobę i używana do celów uwierzytelniania dla usługi online;
20) **UoDE** – ustawa z dnia 18 listopada 2020 r. o doręczeniach elektronicznych;
21) **Usługa zaufania** – świadczona za wynagrodzeniem usługa elektroniczna obejmująca czynności wskazane w art. 3 pkt 16 lit. a-c Rozporządzenia eIDAS;
22) **Ustawa** – ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej

1.3.Definicje Stron KURDE

Nazwa strony	Opis
Dostawca KURDE	KFJ będąca dostawcą KURDE
Dostawca usługi RDE	Dostawca usługi rejestrowanego doręczenia elektronicznego, inny niż dostawca KURDE
Klient	Podmiot publiczny, podmiot niepubliczny (w tym osoba fizyczna), będący nadawcą lub odbiorcą KURDE
Strona ufająca	Klient polegający na zaufaniu do KURDE

1.4.Podstawowe elementy KURDE

1) KURDE składa się z następujących elementów: nadania Przesyłki, doręczenia Przesyłki i wystawienia Dowodów dokonanych czynności:
    a) nadanie Przesyłki, obejmujące następujące kroki:
        i) identyfikację i uwierzytelnienie Klienta realizującego nadanie Przesyłki w Systemie KURDE,
        ii) przekazanie przez Klienta Przesyłki do nadania przez Dostawcę KURDE,
        iii) wystawienie dowodu wysłania przez Dostawcę KURDE,
    b) doręczenie Przesyłki, obejmujące następujące kroki:

i) przekazanie przez Dostawcę KURDE do Klienta w roli odbiorcy informacji o gotowej do odbioru Przesyłce,
ii) identyfikację i uwierzytelnienie Klienta umożliwiające odbiór Przesyłki,
iii) wystawienie dowodu otrzymania przez Dostawcę KURDE,

c) wystawienie dowodów:
i) wysłania Przesyłki - dostępny dla Klienta będącego nadawcą KURDE,
ii) preawizacji (dowód przygotowania Przesyłki do odbioru/dowód o wysłaniu notyfikacji o Przesyłce gotowej do odbioru) - dostępny dla Klienta będącego nadawcą i Klienta będącego odbiorcą,
iii) otrzymania Przesyłki (generowany także w przypadku zaniechania odbioru) - dostępny dla Klienta będącego nadawcą i Klienta będącego odbiorcą.

2) Dostęp do wystawionych Dowodów możliwy jest po uprzednim uwierzytelnieniu się do Skrzynki doręczeń.
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) Dowody w zakresie nadania oraz doręczenia są zabezpieczone pieczęcią elektroniczną oraz znakowane czasem. KFJ udostępnia Klientom dowody wytworzone w procesie świadczenia KURDE przez okres nie dłuższy niż 36 miesięcy od momentu ich wytworzenia.
5) Niezależnie od utraty danych z powodów technicznych lub innych, KFJ zapewnia utrzymanie dokumentów i danych, wynikających z art. 17 Ustawy, przez okres 20 lat od momentu ich wytworzenia.
6) Dostawca KURDE weryfikuje, czy usługi, z którymi współpracuje, są co najmniej usługą rejestrowanych doręczeń elektronicznych.
7) Dostawca KURDE uwierzytelnia wszelkich innych Dostawców usługi RDE przed przekazaniem im treści Klienta lub zaakceptowaniem od nich przekazanych treści Klienta.
8) Dostawca KURDE chroni poufność tożsamości Klienta, zwłaszcza podczas procesu wymiany Przesyłki z innym Klientem.

2.Administracja i repozytorium

2.1. Administracja Polityką

1) KFJ wskazuje Dyrektora KFJ, jako podmiot odpowiedzialny za administrowanie Polityką.
2) Każdorazowa zmiana Polityki wymaga podjęcia uchwały przez Zarząd KFJ. 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 Dyrektor KFJ.
4) W ramach świadczenia KURDE, KFJ 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:
    a) aktualnej i obowiązującej wersji Polityki,
    b) historycznych wersjach Polityki,
    c) Regulaminie,
    d) innych dokumentach przeznaczonych do publikacji na podstawie Polityki, jeśli takie wskazano.
2) Dokumenty umieszczone w repozytorium są publicznie dostępne pod adresem doreczeniaelektroniczne.pl.
3) Wszelkie zmiany Polityki są aktualizowane, 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) W ramach KURDE Dostawca KURDE dokonuje weryfikacji tożsamości nadawcy i adresata bezpośrednio lub polegając na stronie trzeciej. Dopuszcza się następujące sposoby identyfikacji i uwierzytelnienia:

a) za pomocą certyfikatu zaawansowanego podpisu elektronicznego lub zaawansowanej pieczęci elektronicznej, lub
b) stosując metody identyfikacji uznane na poziomie krajowym, które zapewniają równoważną pewność pod względem wiarygodności fizycznej obecności, lub
c) wzajemne uwierzytelnianie z wykorzystaniem bezpiecznego protokołu oraz certyfikatów uznawanych w ramach KURDE, lub
d) zaawansowany podpis elektroniczny lub zaawansowaną pieczęć elektroniczną, lub
e) środek uwierzytelniający o równoważnym poziomie bezpieczeństwa ze wskazanymi powyżej.

2) Identyfikacja elektroniczna przeprowadzana jest przed nadaniem lub doręczeniem Przesyłki.
3) KFJ, 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) 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.
5) KURDE 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.
6) Odpowiedzialność za proces identyfikacji i uwierzytelniania oraz za późniejszy jego nadzór sprawuje Inspektor ds. weryfikacji tożsamości.

4.Zabezpieczenia organizacyjne, operacyjne i fizyczne

1) KFJ posiada wewnętrzny zbiór dokumentów opisujący sposób zarządzania bezpieczenstwem informacji w KFJ Inwestycje. Dokumenty wychodzące w skład zbiory tworzą System Zarządzania Bezpieczeństwem Informacjidotyczący [SZBI].
2) SZBI dotyczy również zarządzania bezpieczeństwem informacji w zakresie KURDE.
3) Każda osoba uczestnicząca w wykonywaniu usługi KURDE jest zobowiązana do zapoznania się i działania zgodnie z zasadami dot. bezpieczeństwa informacji opisanymi w SZBI

4) KFJ 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 KURDE 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 KURDE jest kontrolowany przez pracowników ochrony.
2) Ochrona fizyczna budynków funkcjonuje 24 godziny na dobę.
3) Pomieszczenia wykorzystywane w ramach świadczenia KURDE, w tym także pomieszczenia, w których znajduje się sprzętowy moduł bezpieczeństwa, wyposażone są w system kontroli dostępu do pomieszczeń oraz system sygnalizacji włamania i napadu. Dostęp do pomieszczeń wykorzystywanych w ramach świadczenia KURDE posiadają tylko osoby upoważnione.
4) Weryfikacja uprawnień dostępu do pomieszczeń realizowana jest w oparciu o system kontroli dostępu umożliwiający identyfikacją i rozliczalność osób upoważnionych.

4.1.3. Bezpieczeństwo środowiskowe

1) W przypadku zaniku zasilania podstawowego komponenty techniczne Systemu KURDE przechodzą na zasilanie awaryjne.
2) Środowisko pracy w pomieszczeniach wykorzystywanych w ramach świadczenia KURDE kontrolowane jest w sposób ciągły. 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 Inspektora ds. bezpieczeństwa oraz Administratora sieci.
4) System ochrony przeciwpożarowej, zainstalowany w pomieszczeniach wykorzystywanych w ramach świadczenia KURDE, 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. Szczegółowe zasady postępowania z nośnikami danych, a w szczególności sposób niszczenie nośników wycofanych z użytkowania, są opisane w SZBI.

4.1.5.Niszczenie informacji

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

4.2. Zabezpieczenia organizacyjne

4.2.1.Role zaufane

Osoby sprawujące nadzór nad Systemem KURDE pełnią określone Role zaufane, które zaprezentowane są poniżej:

Dyrektor KFJ

- sprawuje nadzór operacyjny nad zespołem wykonującym usługi KURDE;
- odpowiada za zatrudnienie personelu oraz przygotowanie umów z klauzulami bezpieczeństwa;
- uczestniczy w procesie analizy i szacowania ryzyka;
- uczestniczy w pracach Zespołu ds Incydentów;
- podejmuje decyzję o opublikowaniu poprawki bezpieczeństwa i ustala termin publikacji poprawki;
- zapewnienia zgodności KURDE z prawem oraz standardami normalizacyjnymi;
- wdraża postanowienia Polityki;
- nadzór nad realizacją planu ciągłości działania i jego utrzymaniem;
- zawiadamia Organ Nadzoru o zakończeniu działalności;
- powołuje komisję do zniszczenia nośnika danych, przyjmuje protokół zniszczenia nośnika danych.

Administrator systemu

- sprawuje nadzór operacyjny nad działaniem systemów wykorzystywanych do wykonywania usługi KURDE;
- Proponuje zakres uprawnień do systemów przyznanych osobom uczestniczącym w wykonaniu usługi KURDE;
- przyjmuje zgłoszenia incydentów;
- powołuje Zespół ds. Incydentów;
- uczestniczy w pracach Zespołu ds Incydentów;
- prowadzi bieżącą ocenę istniejących i potencjalnych zagrożeń w zakresie bezpieczeństwa informacji;
- wykonuje ocenę przyczyn i skutków incydentów naruszenia bezpieczeństwa informacji oraz nadzoruje gromadzenie materiału dowodowego;
- przygotowuje propozycje działań korygujących i naprawczych oraz nadzoruje ich wprowadzanie;
- wykonuje okresowy przegląd Polityki Bezpieczeństwa Informacji;
- odpowiada za współpracę z Rządowym Zespołem Reagowania na Incydenty Komputerowe CERT;
- nadzoruje i monitoruje proces automatycznych kopii bezpieczeństwa;
- podejmuje decyzje w sprawie wykonania poprawki bezpieczeństwa;
- zarządza modułem HSM.

Administrator sieci

- sprawuje nadzór operacyjny nad infrastrukturą informatyczną wykorzystywaną do wykonywania usługi KURDE;
- prowadzi Rejestr Incydentów;
- wprowadza dane o incydencie do rejestru incydentów oraz zabezpiecza materiał dowodowy oraz powiadamia Administratora Systemu;
- uczestniczy w pracach Zespołu ds Incydentów;
- w przypadku fałszywych alarmów powiadamia zgłaszającego o zdarzeniu, że zdarzenie nie stanowi incydentu bezpieczeństwa;
- wykonuje procedurę zarządzania mediami i odpowiada za niszczenie nośników danych*;*
- nadzoruje działanie serwera do rejestracji i archiwizacji logów;
- wykonuje procedurę tworzenia kopii zapasowych.

Inspektor ds. bezpieczeństwa

- wykonuje procedurę kontroli bezpieczeństwa w tym dokonuje przeglądu praktyk bezpieczeństwa oraz przeprowadza testy bezpieczeństwa;
- sprawuje nadzór operacyjny nad Systemem Bezpieczeństwa Informacji;
- przyjmuje Wnioski o Przygotowanie Poprawki Bezpieczeństwa;

- przyjmuje zgłoszenia incydentów;
- prowadzi Rejestr Poprawek Bezpieczeństwa;
- analizuje Wnioski o Przygotowanie Poprawki Bezpieczeństwa oraz ocenia konieczność wykonania poprawki bezpieczeństwa;
- uzasadnia decyzję o odrzuceniu wniosku o wykonanie poprawki bezpieczeństwa;
- zleca wykonanie poprawki bezpieczeństwa;
- odpowiada za opracowanie i utrzymanie planów ciągłości działania;
- zarządza modułem HSM, odpowiada za zakup pieczęci i jej unieważnienie;
- przygotowuje i przeprowadza szkolenia pracowników dot. bezpieczeństwa informacji;
- nadzoruje przygotowanie dla pracowników materiały szkoleniowe dotyczących systemu zarządzania bezpieczeństwem informacji.

Inspektor ds. audytu

- odpowiada za organizację audytu zewnętrznego KURDE;
- prowadzi Rejestr dokumentów wchodzących w skład "Zbioru dokumentów opisujących wykonywanie przez KFJ Inwestycje usługi KURDE";
- przyjmuje wnioski o aktualizację dokumentu wchodzącego w skład "Zbioru dokumentów opisujących wykonywanie przez KFJ Inwestycje usługi KURDE";
- w przypadku zaakceptowania wniosku o aktualizację dokumentu wchodzącego w skład "Zbioru dokumentów opisujących wykonywanie przez KFJ Inwestycje usługi KURDE" zleca aktualizację osobie, która jest gospodarzem dokumentu;
- przedstawia zaktualizowane dokumenty do zatwierdzenia Zarządowi KFJ;
- Obsługa zgłoszeń zdarzeń i incydentów;
- Analizowanie zdarzeń i incydentów dotyczących KURDE;
- Rekomendowanie działań naprawczych;
- Kontrola wdrożonych mechanizmów i środków bezpieczeństwa.

Inspektor ds. weryfikacji tożsamości

- przygotowuje i aktualizuje procedurę identyfikacji oraz weryfikacji tożsamości;
- przeprowadza okresowe oceny procedury identyfikacji oraz weryfikacji tożsamości;
- prowadzi bieżącą analizę technologii wykorzystywanych w procesie identyfikacji i weryfikacji tożsamości;
- przeprowadza okresowe oceny działania mechanizmu identyfikacji oraz weryfikacji tożsamości, a w szczególności ocenia czy działania mechanizmu odpowiada aktualnym technologiom używanym przy identyfikacji i weryfikacji tożsamości.

4.2.2.Role zaufane podlegające separacji obowiązków

1) Role zaufane wyodrębnione w ramach Personelu zapobiegają nadużyciom, przy korzystaniu z Systemu KURDE.

2) Każdej osobie odpowiedzialnej za eksploatację Systemu KURDE przydzielono tylko takie prawa, które wynikają z pełnionej przez nią Roli zaufanej i ponoszonej z tego tytułu odpowiedzialności.
3) Rola Inspektora ds. Bezpieczeństwa nie może być łączona z rolą Administratora Sieci ani z rolą Administratora Systemu. Rola Inspektora ds. Audytu nie może być łączona z żadną z pozostałych wymienionych ról zaufanych.

4.2.3.Zarządzanie incydentami

1) KFJ bez zbędnej zwłoki zawiadamia Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL pełniący rolę głównego zespołu CERT w obszarze administracji rządowej, 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.
2) Powyższe obowiązki notyfikacyjne pozostają bez uszczerbku dla obowiązków notyfikacyjnych KFJ 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).
3) W ramach świadczenia KURDE istnieje także procedura wewnętrzna regulująca zarządzanie incydentami.

4.2.4.Zarządzanie ryzykiem

Zarządzanie ryzykiem prowadzone jest zgodnie z ustanowioną w KFJ procedurą zarządzania ryzykiem, w celu dostosowania zabezpieczeń techniczno-organizacyjnych do zidentyfikowanych zagrożeń dla Systemu KURDE.

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:
    a) posiadają pełną zdolność do czynności prawnych,

b) posiadają minimum wykształcenie średnie,
c) zobowiązały się do nieujawniania informacji wrażliwych, z punktu widzenia bezpieczeństwa dostawcy KURDE lub poufności danych Klienta, wynikających z wewnętrznego dokumentu dotyczącego polityki bezpieczeństwa informacji,
d) nie wykonują obowiązków, które mogą doprowadzić do konfliktu interesów pomiędzy urzędem znacznika czasu a działającymi w jego imieniu punktami rejestracji,
e) zapoznały się z wewnętrznymi procedurami KFJ dotyczącymi KURDE,
f) zostały poinformowane o odpowiedzialności karnej w zakresie związanym ze świadczeniem Usług zaufania,
g) 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 KFJ 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:
   a) świadectwa pracy z poprzedniego miejsca zatrudnienia (w przypadku nowej osoby),
   b) dyplomu i świadectwa potwierdzających wykształcenie tej osoby,
   c) 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:
   a) zasad określonych w Polityce,
   b) zasad zawartych w dokumentacji przypisanej roli, którą dana osoba pełni i zakresu obowiązków, które będą wykonywały,
   c) ochrony danych osobowych i ochrony informacji,

d) infrastruktury klucza publicznego,
e) zasad i mechanizmów zabezpieczeń stosowanych w KURDE,
f) oprogramowania systemu komputerowego KURDE,
g) procedur realizowanych po awariach Systemu KURDE lub katastrofach wpływających na System KURDE,
h) zagrożeń i aktualnych praktyk bezpieczeństwa.

2) Szkolenia, o których mowa w ust. 1, są powtarzane co najmniej raz do roku oraz w zależności od potrzeb zawsze wtedy, gdy nastąpiły istotne zmiany w świadczeniu KURDE przez KFJ.

4.2.5.4.Sankcje z tytułu nieuprawnionych działań

1) W przypadku wykrycia nieuprawnionego działania lub podejrzenia o takie działanie ze strony Personelu, Administrator sieci w porozumieniu z Inspektorem ds. bezpieczeństwa może w pierwszej kolejności zablokować dostęp do Systemu KURDE sprawcy takiego zdarzenia.
2) Dalsze postępowanie przeprowadzane jest w porozumieniu z Zarządem KFJ 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

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

1) Polityki,
2) Regulaminu,
3) procedur eksploatacyjnych w zakresie obsługi Systemu KURDE,
4) wzorów umów oraz stosowanych formularzy wniosków,
5) akresu obowiązków i uprawnień wynikających z pełnionej Roli zaufanej.

4.3. Bezpieczna eksploatacja

4.3.1. Rejestrowanie zdarzeń

1) W ramach KURDE rejestrowaniu podlegają w szczególności następujące zdarzenia:
    a) zdarzenia bezpośrednio związane ze świadczeniem Usług zaufania, a w szczególności:
        i) dowody na to, że zasady i warunki świadczenia usługi zostały zaakceptowane przez Klienta,
        ii) czynności systemowe dotyczące dostępu do systemów informatycznych, korzystania z systemów informatycznych i zgłoszeń serwisowych,
        iii) czynności związane z uwierzytelnieniem Klientów KURDE,
        iv) czynności związane z obsługą Klientów, w tym dowody w zakresie rejestrowania nadania i doręczania Przesyłek,
    b) logi systemowe z serwerów i stacji roboczych wchodzących w skład Systemu KURDE,
    c) zdarzenia związane z obsługą techniczną systemu, tj.: błędy i alarmy, rejestr
    wprowadzanych zmian w systemie,
    d) zdarzenia związane z bezpieczeństwem, w tym zmiany związane z wewnętrznym dokumentem dotyczącym polityki bezpieczeństwa informacji, uruchamianiem i zamykaniem Systemu KURDE, awariami Systemu KURDE i awariami sprzętu, działaniami zapory i routera oraz próbami dostępu do Systemu KURDE.
2) Ponadto KFJ zapewnia przechowywanie dowodów w postaci raportów z prowadzonych testów bezpieczeństwa oraz testów penetracyjnych.
3) Logi są zabezpieczone przed modyfikacją, podlegają procedurom tworzenia kopii zapasowych oraz są archiwizowane.
4) 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.
5) Logi w postaci archiwum logów z danego dnia przechowywane są w repozytorium logów przez okres 5 lat.
6) 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 KURDE.

4.3.3. Archiwizacja zdarzeń

1) W ramach KURDE archiwizacji podlegają w szczególności:
    a) dane uwierzytelniające Klienta,
    b) logi operacji w zakresie KURDE, weryfikacji tożsamości Klienta będącego nadawcą i Klienta będącego odbiorcą,
    c) dowody na to, że treść Przesyłki nie została zmodyfikowana podczas transmisji,
    d) tokeny znaczników czasu odpowiadające dacie i godzinie wysyłania i przekazywania oraz modyfikowania treści Przesyłki, stosownie do przypadku,
    e) Polityka oraz jej historyczne wersje,
    f) 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) KFJ zapewnia poufność, integralność i dostępność tworzonych rejestrów zdarzeń.
4) Zapisy dotyczące funkcjonowania KURDE są udostępniane, jeśli jest to wymagane, w celu udokumentowania prawidłowego działania KURDE dla celów postępowania sądowego.

4.3.4. Zakończenie działalności w zakresie KURDE lub przekazanie zadań przez KFJ

1) KFJ, mając na uwadze redukcję wpływu skutków podjęcia potencjalnej decyzji o zakończeniu świadczenia działalności w zakresie KURDE, planuje w szczególności spełnienie obowiązku odpowiednio wczesnego poinformowania o tym organu nadzoru, wszystkich Stron KURDE, kontrahentów i partnerów, z którymi KFJ jest związana umowami, na których wykonanie zakończenie

świadczenia KURDE 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 KURDE przez KFJ określa Plan zakończenia działalności w ramach kwalifikowanej usługi rejestrowanego doręczenia elektronicznego w KFJ Inwestycje Sp. z o.o.
3) Organ nadzoru jest informowany o planach zakończenia działalności w zakresie świadczenia KURDE przez KFJ oraz każdorazowo o każdej jego zmianie.
4) KFJ zobowiązuje się do wykonania następujących czynności:
    a) 1) zapewnienia ciągłości pełnienia roli dostawcy KURDE nie dłużej niż 3 miesiące od dnia poinformowania organu nadzoru, o zamiarze zaprzestania bądź niemożności pełnienia roli podmiotu dostawcy KURDE,
    b) 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,
    c) 3) unieważnienia wszystkich wydanych pełnomocnictw do podpisywania umów o świadczenie KURDE w imieniu KFJ, nie później niż na dzień zakończenia działalności w zakresie świadczenia KURDE,
    d) 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 KURDE.
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 KURDE.
2) Funkcje zabezpieczające systemów komputerowych są realizowane na poziomie systemu operacyjnego, 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 KURDE wyposażone są w następujące funkcje zabezpieczające:
    a) uznaniową kontrolę dostępu,
    b) możliwość prowadzenia audytu zabezpieczeń,
    c) wymuszanie separacji obowiązków wynikających z pełnionych Ról zaufanych,
    d) wymuszanie wylogowania osoby pełniącej Rolę zaufaną po okresie bezczynności,
    e) kryptograficzną ochronę sesji wymiany informacji oraz zabezpieczenia baz danych,
    f) archiwizowanie historii czynności wykonywanych na komputerze oraz danych dla potrzeb audytu,
    g) bezpieczny kanał pozwalający na wiarygodną identyfikację i uwierzytelnienie Ról zaufanych oraz pełniących je osób,
    h) mechanizm odtwarzania kluczy (tylko w przypadku modułów kryptograficznych) oraz systemu operacyjnego i aplikacji,
    i) 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 KURDE sprawuje Inspektor ds. bezpieczeństwa. Zatwierdza on konfigurację Systemu KURDE 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 KFJ podczas przeprowadzania tych testów gwarantują nieprzerwaną pracę Systemu KURDE, integralność jego zasobów oraz zachowanie poufności danych.
3) Kontrola zarządzania bezpieczeństwem ma na celu takie nadzorowanie funkcjonowania Systemu KURDE, 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 KURDE są rejestrowane, to każda z wprowadzonych zmian wymaga dodatkowo zweryfikowania i akceptacji przez przynajmniej dwie osoby pełniące Role zaufane: Inspektora ds. bezpieczeństwa oraz Administratora sieci.

5) System kontroli zmiany informuje uprawnionych pracowników o wystąpieniu modyfikacji w Systemie KURDE i wymaga jej weryfikacji przez osobę inną od tej, która wprowadzała daną zmianę.
6) Aktualna konfiguracja Systemu KURDE, jak również modyfikacje i aktualizacje tego systemu są dokumentowane i kontrolowane. Zastosowane w Systemie KURDE 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 KURDE sprawują specjaliści w roli Administratora sieci.
2) 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.
3) Cała komunikacja w Systemie KURDE jest realizowana za pomocą szyfrowanych kanałów, zabezpieczających przed ingerencją w treść komunikacji.
4) 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.
5) Szczegółowy zakres połączeń pomiędzy poszczególnymi strefami jest opisany w dokumentacji Systemu KURDE i stanowi tajemnicę KFJ.
6) 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.
7) KFJ 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.
8) W przypadku potrzeby zapewnienia wysokiego poziomu dostępu do KURDE, 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. KURDE, łącząc się z innymi Dostawcami usług zaufania oraz systemami zewnętrznymi, zapewnia ich identyfikację w oparciu o mechanizmy sieciowe, tj.: SSL lub IP-SEC.

9) Wszelkie zmiany wprowadzane w urządzeniach sieciowych wymagają wcześniejszej akceptacji Inspektora ds.bezpieczeństwa. Przeprowadzona zmiana zostaje zaimplementowana dopiero po zweryfikowaniu jej przez Administratora sieci i Administratora systemu. W przypadku znaczących zmian w konfiguracji Systemu KURDE, KFJ 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 lub między rozproszonymi komponentami Systemu KURDE, 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.

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) KFJ zapewnia, iż codziennie dokonuje się kontroli aktualności wpisu dostawcy kwalifikowanego znacznika czasu na liście Kwalifikowanych dostawców usług zaufania.

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 KURDE są generowane i przetwarzane w urządzeniach HSM posiadających jeden z certyfikatów:
    a) ISO/IEC 15408 (Common Criteria) dla poziomu EAL4 albo bezpieczniejszego,
    b) ISO/IEC 15408 (Common Criteria) dla poziomu określonego CEN EN 419 221-5:2018 – Protection Profiles for TSP Cryptographic Modules for Trust Services,
    c) FIPS PUB 140-2 dla poziomu 3 albo bezpieczniejszego,
    d) ISO/IEC 19790.

6.Audyt

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

6.1.Częstotliwość i okoliczności oceny

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 KFJ..
2) Zarząd KFJ powołuje zespół osób, w celu przygotowania w terminie określonym w raporcie, pisemnego stanowiska KFJ wobec wszelkich uchybień wskazanych w raportach, przy jednoczesnym określeniu sposobów i terminu usunięcia usterek. Informacja o usunięciu usterek przekazywana jest Inspektrowi ds. audytu
3) W przypadku audytu zleconego przez ministra właściwego do spraw informatyzacji, minister po zapoznaniu się z protokołem i zastrzeżeniami oraz wyjaśnieniami zgłoszonymi przez KFJ 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 KFJ, Inspektor ds. Bezpieczeństwa i innym osobom pełniące Role Zaufania.

7.Inne postanowienia

7.1.Opłaty

Dostawca KURDE pobiera opłatę za świadczenie KURDE zgodnie z cennikiem usług opublikowanym na stronie internetowej doreceniaelektroniczne.pl

7.2.Odpowiedzialność finansowa

1) KFJ potwierdza, że zapewniono wystarczające środki finansowe na obsługę KURDE i wypełnienie wszystkich zobowiązań dotyczących KURDE.
2) Wszystkie uzgodnienia, niezbędne do świadczenia Usługi zaufania, z podwykonawcami, partnerami outsourcingowymi i stronami trzecimi, podlegają umowom i regulacjom obowiązującym w tym zakresie w KFJ.

7.3.Poufność informacji

Personel zatrudniony w KFJ bądź podmioty dokonujące czynności operacyjno-technicznych, w ramach obsługi Systemu KURDE 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 KFJ. W szczególności dotyczy to:

1) informacji wpływającej od/do Klientów KURDE,
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, informacji o administrowaniu Usługami zaufania oraz projektowanymi zasadami rejestrowania.

7.4.Ochrona danych osobowych

KFJ 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 doreczeniaelektroniczne.pl.

7.5.Zgodność z obowiązującym prawem

Funkcjonowanie KFJ w zakresie świadczenia KURDE oparte jest na zasadach zawartych w Polityce oraz obowiązujących na terytorium Polski przepisach prawa.

7.6.Zobowiązania i gwarancje

7.6.1.Zobowiązania KFJ

1) KFJ gwarantuje, że postępuje zgodnie z prawem, a w szczególności:
    a) nie narusza postanowień UoDE wraz z przepisami wykonawczymi,
    b) nie narusza postanowień Standardu,
    c) nie narusza postanowień Rozporządzenia eIDAS, Ustawy wraz z przepisami Wykonawczymi.

7.6.2.Zobowiązania zewnętrznych podmiotów

1) Wszystkie podmioty w tym wszyscy Dostawcy usług zaufania, współpracujące z KFJ, są zobowiązane spełniać wymagania wynikające z Polityki.
2) Świadcząc KURDE w oparciu o innych Dostawców usług zaufania, KFJ zobowiązuje dostawców do spełnienia wymagań bezpieczeństwa wynikających z Polityki.
3) Świadcząc KURDE w oparciu o komponennty innych Dostawców usług zaufania, KFJ zapewnia korzytsanie z komponentu zgodnie z wymaganiami określonymi przez dostawcę komponentu usługi zaufania.
4) Świadcząc KURDE w oparciu o komponennty innych Dostawców usług zaufania, KFJ zapewnia korzytsanie z komponentu zgodnie z wymaganiami bezpieczeństwa i funkjonalności określonymi w polityce i praktykach przez dostawcę komponentu usługi zaufania.

7.6.3.Zobowiązania klientów KURDE

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

7.7.Ograniczenia odpowiedzialności

1) Odpowiedzialność KFJ oparta jest na ogólnych zasadach zawartych w Polityce i Regulaminie oraz jest zgodna z UoDE.
2) KFJ nie ponosi odpowiedzialności finansowej zdefiniowanej w Polityce, wobec innych osób trzecich, niebędących odbiorcami Usług zaufania dostarczanych przez KFJ.

3) W celu nadzoru nad sprawnym działaniem Systemu KURDE, 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 KURDE.

7.8.Odszkodowanie

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

7.9.Procedura wprowadzania zmian

1) Niezależnie od prowadzonych w KFJ audytów, raz w roku odbywa się przegląd obowiązującej wersji Polityki. Personel analizuje 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 KFJ.
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.

8. Podmioty zewnętrzne wspierające KURDE

8.1 Kwalifikowani dostawcy, z którymi współpracuje KFJ w zakresie świadczenia KURDE

1) Timestamp CA, Kingdom of Belgium - Federal Government - Dostawca usługi kwalifikowanego znacznika czasu, wykorzystywanego do znakowania czasem wszystkich zarejestrowanych Przesyłek (w tym dowody wysłania i otrzymania) zgodnie z Polityką.
2) KIR, Poland - Dostawca usługi kwalifikowanej pieczęci elektronicznej wykorzystywanej do zabezpieczenia integralności wszystkich Przesyłek zgodnie z Polityką.

8.2 Inne podmioty zewnętrzne

1) Pomorskie Centrum Przetwarzania Danych (PCPD)- Podstawowe centrum zawierające systemy teleinformatyczne wykorzystywane do świadczenia KURDE. PCPD zapewnia zabezpieczenia fizyczne.
2) Amazon Web Services- Zapasowe centrum zawierające systemy teleinformatyczne wykorzystywane do świadczenia KURDE w tym w szczególności obsługa Backupów KURDE. Amazon zapewnia zabezpieczenia fizyczne.
3) Podmioty pełniące Role Zaufania - Podmioty, z którymi podpisano stosowne umowy niezbędne do pełnienia Roli zaufania w zakresie opisanym w Polityce oraz dokumentach wewnętrznych.