AMT FÜR JUSTIZ
FÜRSTENTUM LIECHTENSTEIN

STIFTUNGSAUFSICHT UND GELDWÄSCHEREIPRÄVENTION

Dokumentnummer	Dokumentdatum	Direktkontakt
AJU / z70.006.03	02/2023	info.zkr.aju@llv.li

Verarbeitungsreglement zum Zentralen Kontenregister

Klassifizierungsstufe (Art. 4 ISchV): Vertraulich

Inhaltsverzeichnis

Dokumentenkontrolle

Version - Datum	***Beschreibung***	***Name***
0.1 - 01.10.2021	*Version 1 erstellt*	*Albert Kaufmann* *Katrin Vidler-Tschabrun* *Miriam Kaufmann*
0.2 - 07.04.2022	*Anpassung Punkt 6.1*	*Martin Alge* *Albert Kaufmann* *Miriam Kaufmann*
0.3. - 27.02.2023	*Entfernung Punkt 2.2 (Übergangsbestimmungen)* *Ergänzung Punkt 6.7 (Rechte der betroffenen Personen)*	*Martin Alge* *Albert Kaufmann* *Daniela Pieber*

1. ALLGEMEINE BESTIMMUNGEN

1.1 Ziel des Verarbeitungsreglements

Das vorliegende Verarbeitungsreglement umschreibt im Sinne von Art. 1 der Verordnung über das Zentrale Kontenregister (ZKRV) insbesondere die Datenverarbeitungs- und Kontrollverfahren sowie den Betrieb des Zentralen Kontenregisters. Es enthält Angaben über den Datenschutz und die Datensicherheit sowie die Zwecke der Datenverarbeitung.

Das Verarbeitungsreglement wird regelmässig aktualisiert und den zugriffsberechtigten Behörden und Kontrollorganen sowie in Auszügen den Banken und Wertpapierfirmen zur Verfügung gestellt.

1.2 Begriffsbestimmungen und Abkürzungen

Im Sinne dieses Verarbeitungsreglements bedeuten:

a) **AI**: Amt für Informatik;
b) **AJU:** Amt für Justiz;
c) **Bankarbeitstage**: die Wochentage Montag bis Freitag, ausgenommen die gesetzlichen Feiertage und die folgenden Tage: Berchtoldstag (2. Januar), Maria Lichtmess (2. Februar), Fastnachtsdienstag, Hl. Josef (19. März), Karfreitag, Hl. Abend (24. Dezember) und Silvester (31. Dezember);
d) **DSGVO**: EU-Datenschutz-Grundverordnung;
e) **DSS**: Datenschutzstelle;
f) **Durch IBAN identifizierbare Zahlungs- oder Bankkonten**: alle Zahlungs- oder Bankkonten, die bei einer Bank oder Wertpapierfirma in Liechtenstein geführt werden und über eine IBAN verfügen;
g) **FIU**: Stabsstelle Financial Intelligence Unit;
h) **FMA**: Finanzmarktaufsicht Liechtenstein;
i) **IBAN**: Internationale Bankkontonummer;
j) **ISchV:** Verordnung über den Schutz von Informationen des Landes (Informationsschutzverordnung);
k) **LLV**: Liechtensteinische Landesverwaltung;
l) **Mutation**: jede Änderung eines im ZKR erfassten oder von den Banken oder Wertpapierfirmen gelieferten Datensatzes;
m) **Schliessfächer**: alle Schliessfächer, einschliesslich Tresore und Tresorräume, die von Banken oder Wertpapierfirmen in Liechtenstein verwaltet werden;
n) **SPG**: Gesetz über berufliche Sorgfaltspflichten zur Bekämpfung von Geldwäscherei, organisierter Kriminalität und Terrorismusfinanzierung (Sorgfaltspflichtgesetz);
o) **SPV**: Verordnung über berufliche Sorgfaltspflichten zur Bekämpfung von Geldwäscherei, organisierter Kriminalität und Terrorismusfinanzierung (Sorgfaltspflichtverordnung);
p) **ZKR**: Zentrales Kontenregister;
q) **ZKRV**: Verordnung über das Zentrale Kontenregister.

Im Übrigen finden die Begriffsbestimmungen von Art. 2 SPG ergänzend Anwendung.

Die in diesem Verarbeitungsreglement verwendeten Personenbezeichnungen gelten für Personen weiblichen und männlichen Geschlechts.

1.3 Zweck des Kontenregisters

Das Kontenregister dient im Rahmen der Bekämpfung von Geldwäscherei, organisierter Kriminalität und Terrorismusfinanzierung der zeitnahen Ermittlung aller natürlichen oder juristischen Personen, die ein durch IBAN identifizierbares Zahlungs- oder Bankkonto oder Schliessfach bei einer Bank oder Wertpapierfirma innehaben oder kontrollieren (Art. 29e Abs. 2 SPG).

1.4 Rechtsgrundlagen

Die Führung und der Betrieb des ZKR stützen sich insbesondere auf folgende Rechtsgrundlagen:

- Gesetz über berufliche Sorgfaltspflichten zur Bekämpfung von Geldwäscherei, organisierter Kriminalität und Terrorismusfinanzierung (Sorgfaltspflichtgesetz, SPG);
- Verordnung über das Zentrale Kontenregister (ZKRV);
- Richtlinie (EU) 2015/849 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung (abgeändert durch Richtlinie (EU) 2018/843);
- Datenschutzgesetz (DSG);
- Datenschutzverordnung (DSV);
- Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, DSGVO).

2. SYSTEMDOKUMENTATION

2.1 Kategorien personenbezogener Daten

Im ZKR werden nachfolgende personenbezogene Daten, die im Zusammenhang mit Zahlungs- oder Bankkonten sowie Schliessfächern stehen, verarbeitet:

a) die IBAN und institutsinterne Kundenstamm-Nummer;
b) das Datum der Kontoeröffnung und allenfalls -schliessung;
c) die Art des Kontos;
d) Angaben darüber, ob es sich um ein nach Art. 35 oder Art. 35a SPG gesperrtes Konto (mangelnde Feststellung und Überprüfung der wirtschaftlich berechtigten Person) oder ein sogenanntes nachrichtenloses Konto handelt;
e) die Währung des Kontos;
f) Angaben über mit dem Konto verbundene Schliessfächer, einschliesslich Schliessfachnummer und Mietzeitraum;

g) hinsichtlich einer natürlichen Person als Vertragspartner:
- Name, Vorname, Geburtsdatum, Wohnsitzadresse, Wohnsitzstaat und Staatsangehörigkeit;
- institutsinterne Personenstammnummer;
- Angabe der genauen Funktion sowie Beginn und gegebenenfalls Ende der Funktionsdauer.

h) hinsichtlich einer juristischen Person als Vertragspartner:
- Name oder Firma, Rechtsform, Sitzadresse, Sitzstaat, Gründungsdatum sowie die Namen der für den Rechtsträger im Verhältnis zum Sorgfaltspflichtigen formell handelnden Organe oder Trustees;
- Gesellschaftsregisternummer des Sitzlandes, sofern eine solche vorhanden ist;
- institutsinterne Personenstammnummer;
- Angabe der genauen Funktion sowie Beginn und gegebenenfalls Ende der Funktionsdauer.

i) hinsichtlich natürlicher Personen, die angeben für den Vertragspartner zu handeln, sind zu den oben angegebenen Daten (siehe g) und h)) für die natürliche und juristische Person zusätzlich folgende Daten anzugeben:
- Bezeichnung und Art (Kardinalität und Umfang) des Verfügungsrechtes;

j) hinsichtlich einer natürlichen Person als wirtschaftlich berechtigter Person:
- Name, Vorname, Geburtsdatum, Wohnsitzadresse, Wohnsitzstaat und Staatsangehörigkeit;
- institutsinterne Personenstammnummer;
- Angabe der genauen Funktion sowie Beginn und gegebenenfalls Ende der Funktionsdauer;
- die Unterscheidungsmerkmale für wirtschaftlich berechtigte Personen nach Art. 3 SPV. Bei Zusammentreffen mehrerer Merkmale (z.B. Stifter nach Art. 3 Abs. 1 Bst. b Ziff. 1 SPV und Kontrolle nach Art. 3 Abs. 1 Bst. b Ziff. 6 iVm Abs. 2 SPV) sind sämtliche Merkmale anzugeben.

k) hinsichtlich einer juristischen Person als wirtschaftlich berechtigter Person:
- Name oder Firma, Rechtsform, Sitzadresse, Sitzstaat, Gründungsdatum sowie die Namen der für den Rechtsträger im Verhältnis zum Sorgfaltspflichtigen formell handelnden Organe oder Trustees;
- Gesellschaftsregisternummer des Sitzlandes, sofern eine solche vorhanden ist;
- institutsinterne Personenstammnummer;
- Angabe der genauen Funktion sowie Beginn und gegebenenfalls Ende der Funktionsdauer;
- die Unterscheidungsmerkmale für wirtschaftlich berechtigte Personen nach Art. 3 SPV. Bei Zusammentreffen mehrerer Merkmale (z.B. Stifter nach Art. 3 Abs. 1 Bst. b Ziff. 1 SPV und Kontrolle nach Art. 3 Abs. 1 Bst. b Ziff. 6 iVm Abs. 2 SPV) sind sämtliche Merkmale anzugeben.

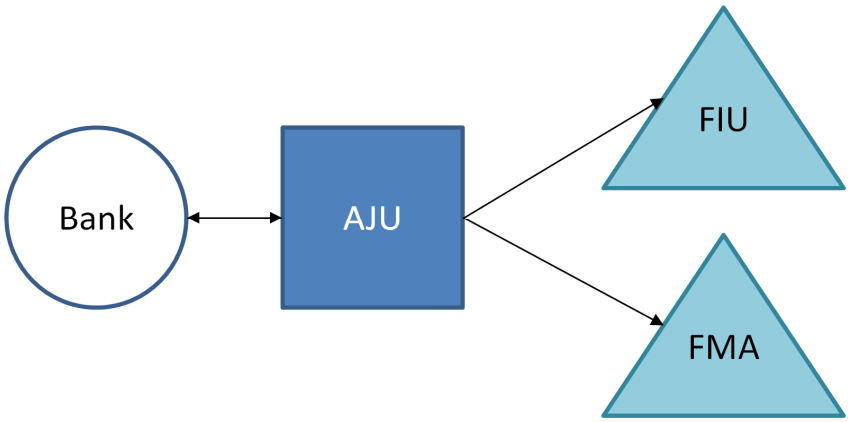
l) ausgenommen von der Meldepflicht sind «Nostro»- und «Vostrokonten»:
Unter «Nostrokonten» sind Konten zu verstehen, die nicht von einer Bank oder Wertpapierfirma, sondern von der Korrespondenzbank geführt werden. Die IBAN der Konten werden daher nicht von der Bank oder Wertpapierfirma, sondern von der Korrespondenzbank als kontoführendes Institut vergeben. Nostrokonten dienen daher ausschliesslich der Schattenbuchhaltung der Bank

oder Wertpapierfirma, welche letztlich mit den Kontobuchungen der Korrespondenzbank abgestimmt werden.
Unter «Vostrokonten» sind Konten zu verstehen, welche die Bank oder Wertpapierfirma für Transaktionen gegenüber ihren Gruppengesellschaften oder als Abwicklungskonten für die Finanzbuchhaltung nutzt, die die Bank oder Wertpapierfirma zum Zwecke der internen Abwicklung benötigt.

2.2 Kategorien der Empfänger der Daten

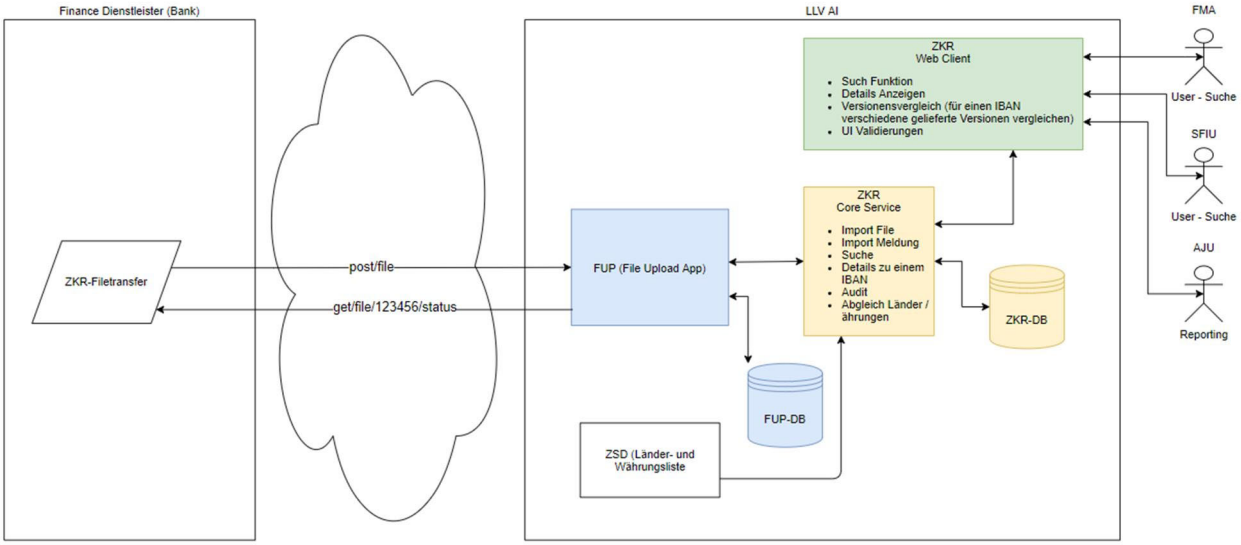
Betreiber des ZKR ist das AJU. Die technische Eingabe bzw. die Übermittlung der Daten an das AJU erfolgt über ein vom AI bereitgestelltes System. Zu diesem System werden der FMA und der FIU im Einzelfall zum Zwecke der Bekämpfung von Geldwäscherei, organisierter Kriminalität und Terrorismusfinanzierung Zugriff gewährt. Das AJU verfügt hingegen über keinen inhaltlichen Zugriff auf die im ZKR enthaltenen Datensätze (vorbehalten bleibt die Erstellung von Berichten an die FMA bei der Feststellung von Mängeln, sog. Reports – siehe Punkt 4.2).

2.3 Struktur der Informationssysteme und Schnittstellen



2.4 Kategorien der bearbeiteten Daten und Datenfelder

Die Schnittstellen der einzelnen datenverarbeitenden Stellen sind die Banken und Wertpapierfirmen, das AJU mit technischer Unterstützung des AI sowie die FIU und die FMA. Die Verarbeitungsvorgänge sind in nachfolgender Skizze abgebildet:

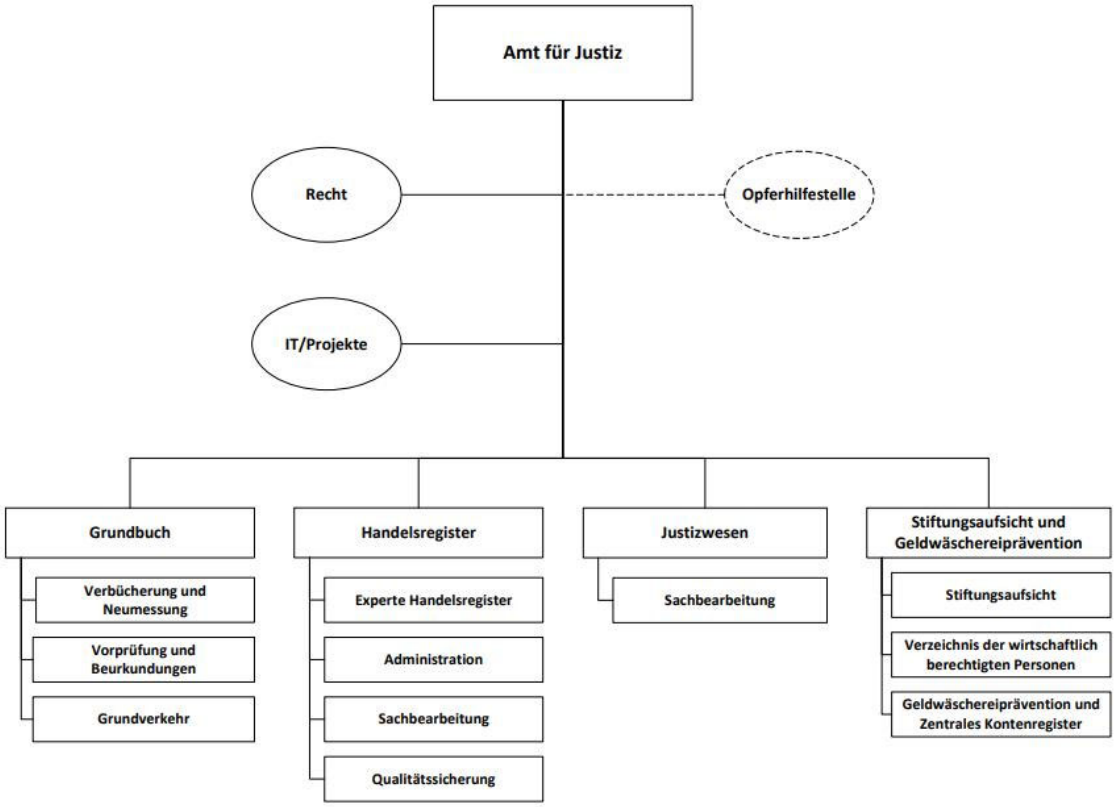


Prozessübersicht – Datenübermittlung in zwei Schritten:

- Schritt 1: Ablieferung der Files seitens Bank oder Wertpapierfirma an LLV FUP-App (allgemeine File Upload Applikation).
- Schritt 2: Übertragung der Files aus der FUP-App in die ZKR-Core-Service-App für den Import der Daten aus dem File in eine eigenständige ZKR-Datenbank (ZKR-DB).

Die einzelnen Datenfelder des ZKR sind in Anhang 1 («Datenstruktur») aufgeführt.

3. ORGANIGRAMM DES AJU



Das ZKR ist im AJU bei der Abteilung Stiftungsaufsicht und Geldwäschereiprävention (STIFA/GWP) angesiedelt.

4. BENUTZER UND DATENÜBERMITTLUNG

4.1 Banken und Wertpapierfirmen

Die Datenübermittlung der Banken und Wertpapierfirmen nach Art. 4 Abs. 1 ZKRV erfolgt über das Hochladen der Datensätze nach Art. 3 ZKRV ins ZKR. Das AJU stellt hierfür mithilfe des AI eine «File Upload Applikation» (FUP) als Schnittstelle zur Verfügung. Die Banken und Wertpapierfirmen übermitteln die Datensätze im Format JSON (Java Script Object Notation).

Die technischen Spezifikationen zur Schnittstelle (FUP) werden vom AJU als YAML-Format (OpenAPI = Standard zur Beschreibung von REST-konformen Programmierschnittstellen) zur Verfügung gestellt. Zusätzlich werden durch das AJU auch die technischen Spezifikationen zum Schema des Files für die Datenübermittlung mitgeliefert (als JSON Schema).

In Ergänzung zu den technischen Spezifikationen erhalten die Banken und Wertpapierfirmen auch eine Übersicht der geforderten Daten in Darstellung einer Excel-Datei (siehe Anhang 1 «Datenstruktur»). Darin werden aus fachlicher Sicht die benötigten Felder für die Datenübermittlung beschrieben, und zwar mit folgenden Kriterien:

- Name (Bezeichnung des Feldes);
- Beschreibung;
- Vorkommen pro IBAN / Element – z.B. einmalig, mehrfach;
- Validierung;
- Pflichtfeld (ja / nein);
- Typ;
- Länge
- Bemerkungen.

Die Datenübermittlung hat in deutscher oder englischer Sprache unter Verwendung des lateinischen Schriftsystems und von arabischen Ziffern zu erfolgen.

4.1.1 Zeitpunkt und Fristen der Datenübermittlung

Die erstmalige Datenübermittlung hat innerhalb von zehn Bankarbeitstagen nach Inkrafttreten der ZKRV am 1. Oktober 2021 (d.h. Fristende: 15. Oktober 2021) durch einen initialen Vollupload in Bezug auf alle Konten und Schliessfächer zu erfolgen.

Hinsichtlich Konten und Schliessfächer, die nach Inkrafttreten der ZKRV eröffnet werden, sind die Daten fortlaufend an dem der Eröffnung folgenden Bankarbeitstag an das ZKR zu übermitteln. Die Daten hinsichtlich der Konten und Schliessfächer, die im Zeitraum der 10-Tages-Frist nach Inkrafttreten der ZKRV (1. bis 15. Oktober 2021) eröffnet wurden, können ebenfalls mit dem erstmaligen initialen Vollupload gemeldet werden.

Nach einem initialen Vollupload finden in weiterer Folge in der Regel nur noch Mutationsuploads bzw. Leermeldungen statt. Die Mutationsdaten, das sind Änderungen bestehender Konten und Schliessfächer oder die Neueröffnung von Konten und Schliessfächern, sind an dem die Mutation folgenden Bankarbeitstag zwischen 0.00 Uhr und 11.00 Uhr zu übermitteln. Massgeblicher Datenbestand bildet der Stand zum Arbeitsschluss des Vortages. Bei Mutationen ist der gesamte Datensatz des betroffenen Kontos oder Schliessfaches, in dem die Mutation erfolgt ist, zu übermitteln.

Erfolgte keine Mutation ist eine sogenannte Leermeldung (siehe unten) zu erstatten.

4.1.2 Leermeldung

Erfolgt an einem Tag keine Mutation oder Änderung der Daten im Stammdatensystem einer Bank oder Wertpapierfirma, hat die Bank oder Wertpapierfirma am darauffolgenden Bankarbeitstag mit dem Mutationsupload trotzdem eine Meldung über die Schnittstelle zu übermitteln. Eine solche Meldung wird als Leermeldung bezeichnet.

Dafür erstellt die Bank oder Wertpapierfirma einen Datensatz, der nur mit den geforderten Metadaten ohne weitere Kontodaten übermittelt wird.

Die Metadaten werden in den technischen Spezifikationen (JSON Schema) beschrieben und sind nachfolgend zusammengefasst:

- „UUID“ – Universally Unique Identifier (wird von der Bank/Wertpapierfirma generiert);
- „date“ – Gültigkeitsdatum (per Datum der Mutation);
- „deliverType“ – Liefertyp (z.B. Vollupload, Mutationsupload);
- „IBANCounts” – Anzahl übermittelter Konten;
- „bank“ – mit „name“ und „CRNumber“ (Handelsregisternummer der Bank/
  Wertpapierfirma).

4.2 Uploadmeldungen

Nach erfolgter Datenübermittlung erfolgt eine systemseitige Rückmeldung («Uploadmeldung») zum Stand der Übermittlung. Diese Uploadmeldung ist von den Banken und Wertpapierfirmen mittels Abrufverfahren zu überprüfen und die Überprüfung zu dokumentieren. Das AI hat für die Datenübermittlung im ZKR geeignete Systemrückmeldungen vorzusehen.

Die Systemrückmeldungen beim Upload eines Datensatzes können durch die Bank und Wertpapierfirma laufend abgefragt werden. Neben dem Status werden hier auch die benötigten Informationen zum Upload angezeigt.

Die Uploadmeldungen umfassen sohin folgende Informationen, die auch in den Spezifikationen (YAML-Datei) zur Verfügung gestellt werden, die die Banken und Wertpapierfirmen erhalten:

- Status – Prozessschritt:
  (1) – file saved (Beschreibung: file is stored in the system);
  (2) – processing file (Beschreibung: processing file);
  (3) – processing finished (Beschreibung: processing finished and all datasets are valid);
  (4) – processing failed (Beschreibung: file is misformatted and refused);
  (5) – processing finished with warnings (Beschreibung: at least one dataset is invalid but stored);
  (6) – processing finished with errors (Beschreibung: at least one dataset is invalid and not stored);
  (7) – general error (Beschreibung: file cannot be processed);
  (8) – processing failed with metadata errors (Beschreibung: metadata are incomplete or wrong, file refused).

- Weitere Statusinformationen (Validierung):
  Ab dem Prozessschritt (2) wird der Upload bzw. das File an das ZKR für die Validierung des Datensatzes übergeben. Die Auswertung erfolgt gemäss den Validierungsregeln, die im Anhang 2 zu diesem Reglement aufgeführt sind.
  Je nach Ergebnis der Auswertung resultiert aus dem Prozess ein unterschiedlicher Status, der angezeigt wird (Status zwischen (3) und (8) oben). Die Banken und Wertpapierfirmen erhalten hierbei immer auch die

Informationen zum Status als Hinweis darauf, wo im Datensatz der Fehler aufgetreten ist. Die Banken und Wertpapierfirmen erhalten folgende zusätzlichen Angaben:

- UUID – zur Identifikation, um welches File es sich handelt (inkl. der Anzahl der im File gelieferten Datensätze / IBANs sowie den fehlerhaften Datensätzen);
- IBAN (Datensatz im File, der betroffen ist);
- Fehlercode und Fehlerbeschreibung.

Sofern es zu einer Uploadmeldung mit den Statusinformationen (4) bis (8) kommt, haben die Banken und Wertpapierfirmen die fehlerhaften Datensätze bei der nächsten Meldung (in der Regel am darauffolgenden Bankarbeitstag) mittels der Mutationsmeldung zu korrigieren und sicherzustellen, dass keine Mutationen verloren gehen (Korrekturupload). Ein solcher Korrekturupload ist durch die Bank oder Wertpapierfirma entsprechend zu kennzeichnen.

Die Uploadmeldungen mit den Statusinformationen (3) bis (8) werden den Banken und Wertpapierfirmen sowie dem AJU zur Verfügung gestellt. Das AJU hat diese Meldungen gemäss den Vorgaben des SPG und der ZKRV in regelmässigen Abständen an die FMA weiterzuleiten (Reports). Diese Uploadmeldungen sind zudem in der Detailansicht für die zuständigen Behörden jederzeit sichtbar.

4.2.1 Überprüfung der Datenübermittlung und Vorgehen bei Systemfehlern

Entsprechend der zuvor beschriebenen Vorgehensweise haben Banken und Wertpapierfirmen die korrekte Übermittlung sowie die Korrektheit der Daten selbst zu überprüfen.

Bei Systemfehlern, die nicht gleichentags korrigiert werden können, ist unverzüglich das AI zu informieren und sicherzustellen, dass keine Daten verloren gehen.

Neben der bestehenden Verpflichtung fehlerhafte Datensätze selbst zu korrigieren, kann das AJU in begründeten Fällen gegenüber Banken und Wertpapierfirmen unter Setzung einer angemessenen Frist (in Abhängigkeit der Datenmenge und Komplexität) einen Korrekturupload in Bezug auf alle bei einer Bank oder Wertpapierfirma geführten Konten und Schliessfächer anordnen. Eine solche Anordnung kann den gesamten Datenbestand (aktuell und historisch) einschliesslich aller Mutationen seit dem Inkrafttreten der ZKRV betreffen oder auf einzelne Datensätze beschränkt sein. Datensätze in Bezug auf Konten und Schliessfächer, die vor mehr als zehn Jahren oder vor Inkrafttreten der ZKRV saldiert wurden, müssen jedoch nicht übermittelt werden. Die Voraussetzungen für eine Anordnung durch das AJU liegen insbesondere dann vor, wenn Datensätze wiederholt vorschriftswidrig, unvollständig oder verspätet übermittelt wurden.

4.2.2 Datenpflege

Im ZKR erfasste Daten sind mit Ausnahme der im Gesetz vorgesehenen Löschung nicht mehr abänderbar.

Banken und Wertpapierfirmen, die einen fehlerhaften Datensatz an das ZKR übermittelt haben, müssen dies im korrigierten Mutationsdatensatz in geeigneter Weise kennzeichnen.

4.3 Aufbewahrungsdauer von Daten

Die Daten im ZKR sind 10 Jahre nach Beendigung der Geschäftsbeziehung mit der meldepflichtigen Bank oder Wertpapierfirma zu löschen.

Protokolldaten sind immer 10 Jahre nach erfolgter Datenverarbeitung zu löschen.

5. DATENVERARBEITUNG

5.1 Datenübernahme

Die Datenübernahme der einzelnen Schnittstellen erfolgt über die zuvor beschriebenen Prozesse. Die von der Bank in das ZKR hochgeladenen Daten sind mit Ausnahme der vorgesehenen Löschung nicht veränderbar.

5.2 Datenweitergabe

Daten, die im ZKR verarbeitet werden, dürfen nur für Zwecke der Bekämpfung von Geldwäscherei, organisierter Kriminalität und Terrorismusfinanzierung weitergegeben werden. Die Weitergabe der Daten kann allenfalls im Rahmen der nationalen und internationalen Amtshilfe erfolgen und richtet sich nach den jeweils anwendbaren Spezialgesetzen.

5.3 Verarbeitung zu statistischen Zwecken

Eine Datenverarbeitung zu statistischen Zwecken ist ausgeschlossen

6. DATENSICHERHEIT, TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

6.1 Grundsätzliches

Die organisatorischen und technischen Massnahmen zur Datensicherheit richten sich grundsätzlich nach den Bestimmungen der Art. 47 Bst. f und Art. 70 Abs. 2 DSG sowie der jeweils aktuell gültigen Version des Informatik-Reglements des Amtes für Informatik.

6.2 Datensicherung

Die Daten befinden sich ausschliesslich im internen Netz der LLV und werden dort gesichert.

Die Wiederherstellung der Datenkonsistenz und Datenintegrität auf dem Datenbanksystem nach einem Datenverlust oder dem Ausfall von Systemkomponenten ist garantiert.

6.3 Verschlüsselung

Die Übermittlung sämtlicher Daten zwischen dem Stammdatensystem der Banken/
Wertpapierfirmen und dem ZKR erfolgt auf einem verschlüsselten Kanal. Die Kommunikation erfolgt mittels Aufbaus einer Transportschichtsicherheit (TLS), die für die Identifikation und Authentifizierung der Kommunikationspartner auf Basis asymmetrischer Verschlüsselungsverfahren und Public-Key-Kryptografie aufgebaut ist. Zusätzlich wird eine Zwei-Wege-Authentifizierung (Mutual TLS) vorausgesetzt, damit der Verbindungsaufbau erst nach erfolgter Authentifizierung des Endpunktes/Clients möglich ist.

Zusätzlich wird noch eine Authentifizierung und Autorisierung via eines Identity Providers (Keycloak) verlangt (unter Verwendung eines Java Web Tokens (JWT) und dem Protokoll OAuth 2.0 mit Client Credential Flow).

Die Datenübermittlung erfolgt in zwei Schritten (siehe Punkt 2.3). Dabei befinden sich die FUP und der ZKR-Core-Service im LLV Core Netz. Dies hat zur Folge, dass sich die von den Banken und Wertpapierfirmen gelieferten Daten zu keinem Zeitpunkt ausserhalb des gesicherten und kontrollierten Bereichs befinden.

Der Zugriff seitens FMA und FIU auf die Daten in der ZKR-Datenbank (nur lesend) findet über den ZKR-Web Client statt und ist nur über das interne LLV-Netzwerk möglich. Der Zugriff erfolgt mittels Standard HTTPS Requests. Für Benutzer Authentifizierung und Autorisierung kommt Keycloak mit der Verwendung vom JWT (Java Web Token) und OAuth 2.0 Standard Authorization Code Flow zum Einsatz.

6.4 Massnahmen zum Schutz der Daten

Die gesamte LLV inklusive des AJU, AI, FIU und der FMA verfügen über eine Zugangskontrolle, sodass der Zugang durch Unbefugte zu den Einrichtungen, in welchen die Daten verarbeitet werden, ausgeschlossen ist.

Aufgrund der Vergabe von Berechtigungen in den jeweiligen Behörden ist der Zugriff auf die verarbeiteten Daten durch Unbefugte ausgeschlossen. Die Zugriffsberechtigten werden einer Personensicherheitsüberprüfung unterzogen. Zusätzlich werden Anträge für Zugriff auf das ZKR ausschliesslich nach dem „need-to-know-Prinzip“ bewilligt und eine Bedarfsprüfung durchgeführt. Das Lesen der Daten ist nur innerhalb des LLV-Netzwerkes möglich, sodass der protokollierte Zugriff, welcher eine Identifikation der zugriffsberechtigten Person erfordert, nicht ausserhalb der Einrichtungen der LLV möglich ist. Eine Veränderung der Daten ist nicht möglich und ein Transport der Daten ist nicht vorgesehen.

Die beschriebenen technischen und organisatorischen Massnahmen gewähren daher vollständigen und unbedingten Schutz der Daten.

6.5 Aufsicht und Zuständigkeiten

6.5.1 Betrieb des ZKR

Dem AJU obliegt der Betrieb des ZKR. Ihm obliegen:

a) die Überprüfung der Vorschriftsmässigkeit, technischen Vollständigkeit und Rechtzeitigkeit der Datenübermittlung;
b) die Anordnung von „Korrekturuploads“;
c) die Berichterstattung bei Feststellung von Mängeln an die FMA;
d) der Erlass eines Verarbeitungsreglements und die Veröffentlichung auf seiner Internetseite;
e) die Erteilung der Zugriffsrechte.

6.5.2 Technischer Betrieb des ZKR

Für den technischen Betrieb und den Systemunterhalt ist das AI verantwortlich. Dem AI obliegen insbesondere:

a) die Einrichtung einer Schnittstelle zur Datenübermittlung;
b) die Entgegennahme von Meldungen über Systemfehler und die Einrichtung von «Uploadmeldungen»;
c) die Einrichtung der Zugriffsberechtigungen.

6.5.3 Vollzug

Die FMA überprüft die Reports des AJU und trifft gegebenenfalls die zur Herstellung des rechtmässigen Zustandes erforderlichen Massnahmen. Dies inkludiert den Erlass von Verfügungen und die Anordnung von Vor-Ort-Kontrollen. Ferner obliegt ihr die Ahndung von Übertretungen nach Art. 31 Abs. 1 Bst. s^{ter} SPG.

6.5.4 Ansprechpersonen

Als erste Anlaufstelle für Angelegenheiten und Probleme im Zusammenhang mit dem ZKR fungiert das AJU (E-Mail: info.zkr.aju@llv.li). Dies gilt insbesondere auch für die Themenbereiche der Benutzerverwaltung für die Behörden oder die Lieferung von Zertifikaten (Public Zertifikat) bei Erneuerungen.

Sofern es sich um technische Themenstellungen oder Probleme handelt, die vom AJU nicht beantwortet bzw. bearbeitet werden können, wird das AJU die jeweilige Anfrage an den zuständigen Applikationsmanager beim AI weiterleiten.

6.6 Meldepflicht

Werden Schwachstellen bzw. Systemfehler von den Benutzern, den Kontrollorganen oder dem AI beobachtet, so sind diese zu dokumentieren und unverzüglich dem AJU (E-Mail: info.zkr.aju@llv.li) schriftlich mitzuteilen.

6.7 Rechte der betroffenen Personen

Auskunftsrecht

Auskunftsersuchen über die Rechtmässigkeit der Verarbeitung der Daten betroffener Personen sind an die DSS zu richten. Diese überprüft die Rechtmässigkeit der Daten insbesondere die Dauer der Speicherung, die Aktualität der Daten und die Rechtmässigkeit allfälliger Einsichtnahmen.

In weiterer Folge teilt die DSS der gesuchstellenden Person in einer stets gleich lautenden Antwort mit, dass entweder keine personenbezogenen Daten über sie unrechtmässig verarbeitet werden oder dass sie bei Vorhandensein allfälliger Fehler in der Datenverarbeitung deren Behebung angeordnet hat.

Die betroffene Person kann vom Verwaltungsgerichtshof eine Überprüfung der Mitteilung oder der verfügten Massnahmen verlangen. Dieser hat in einer immer gleich lautenden Antwort mitzuteilen, dass die Prüfung im begehrten Sinne durchgeführt wurde.

Die DSS kann auch ohne Anlassfall eine Überprüfung der Datenverarbeitung bei den zugriffsberechtigten oder registerführenden Behörden durchführen.

Eine Auskunftserteilung über eine Einsichtnahme ins ZKR der zugriffsberechtigten Behörden ist verboten.

Hinsichtlich der weiteren Rechte betroffener Personen wird auf die Datenschutzhinweise zum ZKR verwiesen.

Vaduz, 27. Februar 2023

Amt für Justiz

FÜRSTENTUM LIECHTENSTEIN
AMT FÜR JUSTIZ

Dr. Martin Alge
Amtsleiter