KLARA
Macht dein Büro einfach.

GEBÜV-KONFORME ARCHIVIERUNG MIT DEM KLARA eARCHIV

Dokumentation für Kunden

Version 1.0, Februar 2023

Inhaltsverzeichnis

1. Einleitung

Dieses Dokument dient als Handbuch für den GeBüV-konformen Betrieb des elektronischen Archivs mit dem Produkt «eArchiv» der KLARA Business AG.

Dieses Dokument ist keine Gebrauchsanleitung für das Produkt «eArchiv» sondern es werden lediglich die GeBüV-konformen Vorgehen aufgeführt. Im Weiteren werden organisatorische Vorgaben und Empfehlungen dargestellt, die für einen GeBüV-konformen Einsatz erforderlich sind oder berücksichtigt werden sollten.

1.1. KLARA und eArchiv

Lohnabrechnungen, Versicherungen der Mitarbeitenden, Arbeitszeugnisse, Krankheits- und Unfallmeldungen oder Buchhaltung rauben Kleinunternehmern wie auch Privathaushalten viel Zeit und Nerven. Wertvolle Zeit, die man viel lieber ins Tagesgeschäft oder in die Freizeit investieren möchte. KLARA hat sich mit diesem Problem auseinandergesetzt und eine innovative Lösung gefunden: KLARA nimmt weit mehr als nur den administrativen Aufwand ab und macht so das Büro einfach. Ausserdem ist KLARA zertifizierter Google Partner.

Kostenpflichtige Zusatzangebote unterstreichen dieses Kernangebot und helfen den Kunden, das Geschäft noch produktiver zu führen. Eines dieser kostenpflichtigen Zusatzangebote ist «eArchiv».

Das Proudukt KLARA eArchiv ermöglicht den Kunden von KLARA eine nach GeBüV konforme digitale Archivierung. Für einen GeBüV-konformen Einsatz von «eArchiv» ist mindestens der Einsatz der Variante «Basic» erforderlich. Wahlweise kann die Variante «Plus» abonniert werden, welche über ein zusätzliches Zugriffsmanagement verfügt, damit die Berechtigungen auf Dokument- oder Ordnerebene verwaltet werden können.

1.2. GeBüV

Die Verordnung über die Führung und Aufbewahrung der Geschäftsbücher (GeBüV) vom April 2002 (Stand vom 1. Januar 2013) stützt sich auf Artikel 958f Absatz 4 des Schweizerischen Obligationenrechts. In der GeBüV sind die zu führenden Bücher angeführt und es werden allgemeine Grundsätze der Führung und Aufbewahrung festgeschrieben. Darüber hinaus werden Grundsätze für die ordnungsgemässe Aufbewahrung im Speziellen sowie Angaben zu zulässigen Informationsträger- gern und Verfahren gemacht. GeBüV ist in fünf Abschnitte gegliedert:

1. Zu führende Bücher – Hauptbuch und, je nach Art und Umfang des Geschäfts, auch Hilfsbücher
2. Allgemeine Grundsätze ordnungsgemässer Führung und Aufbewahrung der Bücher, Integrität, Dokumentation
3. Grundsätze für die ordnungsgemässe Aufbewahrung – Sorgfaltspflicht, Verfügbarkeit, Organisation, Archiv
4. Informationsträger – Zulässige Informationsträger, Überprüfung und Datenmigration
5. Schlussbestimmungen - Inkrafttreten und Aufhebung bisherigen Rechts

Dokumentation zu GeBüV ist im Internet über den folgenden Link abrufbar: https://www.admin.ch/opc/de/classified-compilation/20001467/index.html

2. Betriebsempfehlungen von eArchiv

Nachfolgend werden betriebsorganisatorische Empfehlungen festgehalten, welche bei Verwendung von «eArchiv» zu beachten sind. Diese Anforderungen können innerhalb des KLARA Kernangebotes abgebildet werden.

2.1. Archivformate

Das KLARA eArchiv kann eine Vielzahl von verschiedenen Formaten speichern und archivieren. Für die Langzeitarchivierung und die Archivierung nach GeBüV ist es wichtig Langzeitarchiv-Formate zu verwenden.
Das KLARA eArchiv garantiert die GeBüV-konforme Archivierung ausschliesslich mit dem Format «PDF/a» und konvertiert deshalb alle PDF-Dateien in PDF/a um.

2.2. Authentisierung und Autorisierung

Die Vergabe und Verwaltung von allgemeinen Zugriffsberechtigungen können ausschliesslich innerhalb von KLARA erfolgen. Für die Vergabe und Verwaltung von Zugriffsberechtigungen auf Dokument- resp. Ordnerebene wird das Angebot «eArchiv» in der Variante «Plus» benötigt.

Das Identity Management der User kann ausschliesslich ausserhalb von KLARA durch den Kunden vorgenommen werden. Dahingehend ist der Kunde für die entsprechende Organisation und Dokumentation verantwortlich oder kann auf entsprechenden Vorgaben, Richtlinien und Dokumentationen zu verweisen.

Im Weiteren ist darauf zu achten, dass alle natürlichen Personen, die KLARA als User einer Firma nutzen, ein eigenes, personenbezogenes Benutzerprofil erhalten und als User einer Firma innerhalb des KLARA Kernangebotes erfasst sind. Anderenfalls ist nicht sichergestellt, dass anonyme Zugriff verhindert werden.

Der Kunde ist für die Organisation, Dokumentation und Verwaltung der Zugriffsberechtigungen verantwortlich, insbesondere für die Entnahme der Zugangsrechte beim Austritt eines Mitarbeiters.

Alle relevanten Kennworte zu Administrations-Benutzerprofilen (User) für den Zugriff auf KLARA und die Verwaltung innerhalb KLARA sind durch die Kunden über ein dokumentiertes Verfahren zu verwalten. Die Nutzung der Benutzerprofile resp. Kennworte ist, soweit es sich um kritische Informationszugänge handelt, im Vier-Augen-Prinzip zu organisieren. Insbesondere gilt dies auch für das Zurücksetzen von Kennworten.

Die Vergabe von Administrations-Benutzerprofilen (User) muss regelmässig innerhalb des KLARA Kernangebotes durch den Kunden kontrolliert und gegebenenfalls angepasst werden.

Jeder Nutzer von KLARA der auf GeBüV-konform archivierte Dokumente (bzw. auf das System selbst) zugreifen können soll, muss zwingend innerhalb des KLARA Kernangebotes registriert sein. KLARA kennt keine anonymen Benutzer.

2.3. Aufbewahrungsfristen

Die Fristen für die Aufbewahrung von Archivdokumenten nach GeBüV sind durch den Kunden festzustellen. Zu beachten ist, dass aus anderen regulatorischen oder gesetzlichen Vorgaben Fristen resultieren können, die über die Anforderungen des GeBüV hinausgehen (z.B. Produkthaftpflicht). Die Einhaltung der Fristen obliegt der Verantwortung des Kunden und wird nicht durch «eArchiv» geregelt / überprüft.

Mögliche Gesetze mit Auswirkungen auf die Aufbewahrungsfristen:

- Datenschutzgesetz
- Gesetz über die zweite Säule der Pensionsfonds
- etc.

2.4. Integritätsüberprüfung

Der Kunde ist verpflichtet beim Hochladen einer Datei aus einer externen Quelle zu überprüfen, dass die Integrität erhalten blieb, bevor die Datei archiviert wird. KLARA führt im eArchiv bei jedem User Login (max. 1x pro Tag) ein Integrity Check durch, der wie folgt abläuft:

- Prüfung der Gültigkeit der Signatur von Dokumenten durch Vergleichen von Hashes der Anfrage mit einem neu generierten des Dokumentes bei 100 Dokumenten
- Prüfung, ob die Dokumente entschlüsselt werden können
- Prüfung, ob jedes Dokument eine digitale Signatur hat
- Überprüfung der Übereinstimmung der digitalen Signaturen
- Tritt bei dieser Überprüfung ein Fehler auf wird ein internes Alarming ausgelöst, um die Problemursache zu identifizieren und diese zu beheben
- Danach werden die Hashes der betroffenen Dokumente wieder kalkuliert damit die Signatur sichergestellt werden kann

2.5. Exportieren von Dokumenten

KLARA stellt beim Exportieren von Dokumenten aus dem Archiv Originalformate, elektronische Signaturen und die Logfiles zur Verfügung.

Die exportierten Daten stehen dem Kunden für 14 Tage mittels persönlichem Download-Link zur Verfügung und können nur mittels eines vormalig – durch ein Administrations-Benutzerprofil (User) – definiertem Passwort entschlüsselt werden.

Im Falle eines Exports der Archivdaten empfiehlt KLARA eine Überprüfung der heruntergeladenen Dokumente auf Vollständigkeit und Korrektheit.

3. Technische Merkmale

3.1. Datenhaltung

Alle Dokumente in Originalformaten (PDF/A), weitere Dokumente und Dokumentinformationen und Logfiles werden durch KLARA in Google Cloud Storage in der Schweiz mehrfach redundant gespeichert. Die Dokumente in Originalformaten werden dabei Kunden-spezifisch verschlüsselt, um diese vor unerlaubten Einsichten und Veränderungen zu schützen.

Die Sicherung der Daten erfolgt mit dem üblichen Backup -Verfahren, welche die KLARA Business AG ohnedies bereits einsetzt.

3.2. Backups

Das Backup der Daten erfolgt auf mehreren Wegen:

Schnappschüsse
- Es wird täglich ein Snapshot vom Datenträger der Datenbank erstellt. Diese Snapshots haben eine Lebensdauer von 14 Tagen.

Standby-Datenbank
- WAL-Dateien aus der Hauptdatenbank werden im WAL-Speicher gespeichert
- Eine sekundäre Standby-Datenbank liest die WAL-Dateien aus dem WAL-Speicher und wird damit mit auf dem neuesten Stand gehalten.

Voll-Backups auf Backup-Server
- Wöchentliche Voll-Backups werden von der Standby-Datenbank erstellt und an den Backup-Server ausgeliefert. Die WAL-Dateien werden vom WAL-Speicher auf den Backup-Server synchronisiert

Sicherung der Backups

- Alle WAL- und Backup-Dateien werden auch mit einem GCP-Storage-Bucket synchronisiert, der sich in einem separaten GCP-Projekt befindet.

3.3. Wiederherstellen

Je nach Problem, mit dem KLARA konfrontiert ist, finden die folgenden Wiederherstellungsverfahren statt:

Die Daten (Festplatte) der Hauptdatenbank sind beschädigt.

- Die Daten des Standby-Datenbankservers werden dupliziert und für die Hauptdatenbank verwendet.

Die Daten (Datenträger) der Haupt- und der Reservedatenbank sind beschädigt.

- Der letzte Snapshot der Festplatte der Hauptdatenbank wird als Startpunkt verwendet.
- Alle seit diesem Snapshot erzeugten WALs werden angewendet.
- Die resultierende Datenplatte wird dupliziert und für den Standby-Server verwendet.

Die Daten (Festplatte) der Haupt- und der Standby-Datenbank sind beschädigt, und alle Snapshots sind ebenfalls beschädigt.

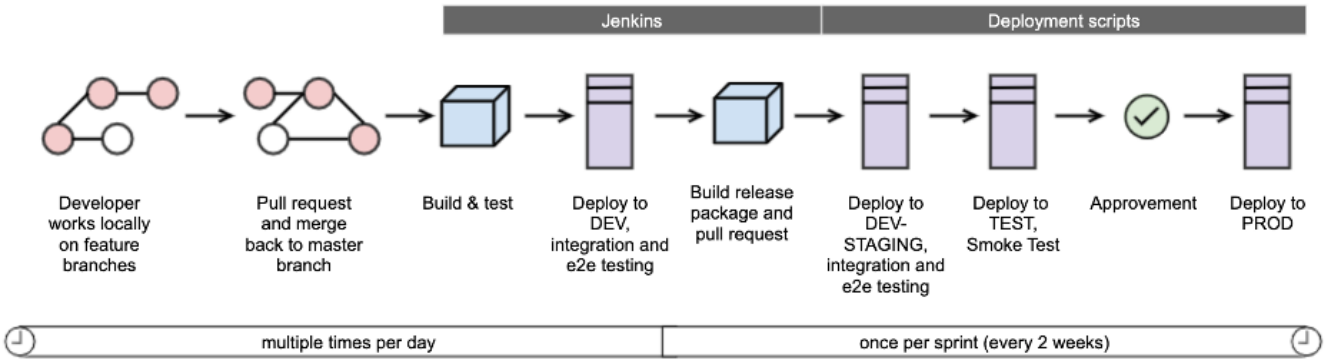
- Die letzte Vollsicherung der Datenbank wird als Ausgangspunkt genommen.
- Alle WALs, die seit dieser Sicherung erstellt wurden, werden angewendet.
- Die resultierende Datenplatte wird dupliziert und für den Standby-Server verwendet.

Alle Daten werden auf dem GCP-Projekt beschädigt.

- Haupt- und Standby-Datenbankserver werden neu aufgesetzt
- Die letzte Vollsicherung der Datenbank im separaten GCP-Projekt wird als Ausgangspunkt genommen. Alle seit dieser Sicherung erzeugten WALs werden vom separaten GCP-Projekt übernommen.

3.4. Changeprozess

Bevor eine neue Version einer Software bei KLARA in Betrieb genommen wird, durchläuft sie mehrere Testphasen, um sicherzugehen, dass eine Abwärtskompatibilität und ein fehlerfreier Betrieb möglich sind. Die nachfolgende Abbildung zeigt das Vorgehen bei KLARA auf:



4. Varianten

4.1. Basic

«eArchiv» umfasst in der Standardauslieferung «Basic» eine Reihe von Eigenschaften, die einen nachvollziehbaren, den üblichen Anforderungen an die rechtskonforme Aufbewahrung entsprechenden Betrieb eines elektronischen Dokumentenarchivs ermöglichen.

Zu den Features, die im Standardumfang von «eArchiv» enthalten sind, gehören die folgenden Möglichkeiten:

- Alle Dokumente werden manipulationssicher (verschlüsselt) gespeichert und können nur durch den Kunden eingesehen werden
- Alle Änderungen und Zugriffe an Dokumenten (Metadaten) werden aufgezeichnet und gespeichert
- Die Änderungen werden in einem Blockchain-Verfahren miteinander «verknüpft»
- Alle Änderungen am Dokument werden dem User als History im User-Interface angezeigt
- Jedes Dokument wird mit einer externen Signatur versehen und Informationen dazu dem User auf dem User-Interface angezeigt
- Regelmässige Integritätsprüfung gemäss Integritätsüberprüfung

4.2. Plus

Die Zusatzoption «Plus» umfasst alle Features, welche in der Standardauslieferung «Basic» enthalten sind. Zusätzlich bietet diese Option jedoch noch die Möglichkeit, Zugriffsrechte auf Dokument- oder Ordnerebene zu definieren. Dies wurde wie folgt umgesetzt:

1. Jedem Geschäftsobjekt (Dokument oder Ordner) können eine oder mehrere Sicherheitsklassen zugewiesen werden
2. Jedem User können eine oder mehrere Sicherheitsklassen zugewiesen werden
3. Ein User hat Zugang zu den Geschäftsobjekten, die mindestens einer Sicherheitsklasse entsprechen, die ihm zugewiesen wurde.
4. Der Administrator des Firmenprofils in KLARA Business hat immer Zugriff auf alle Dokumente.

5. Aufzeichnungen

Änderungen an Dokumenten und Ordnern werden durch die Erstellung von Ereignissen nachverfolgt, welche die Änderungen an den Metadaten des Dokuments oder Ordners dokumentieren. Folgende Metadatenänderungen werden nachverfolgt und im Ereignis speziell erwähnt (Werte sind verschlüsselt):

- Änderungen des Dokumenttyps
- Änderungen an der Ordnerverknüpfung eines Dokuments
- Änderungen von Tags

Ein Ereignis besteht aus den folgenden Daten:

- Id (eindeutige ID)
- auditData (Änderungen von Dokumenttyp, Ordnerverknüpfung oder Tags)
- eventDateTime (Zeitstempel)
- eventDescription (Benutzeraktion)
- eventFingerprint (berechneter Hashwert)
- eventStatus (erfolgreich oder fehlgeschlagen)
- eventSubType (Objekt; Dokument, Datei, Metadaten usw.)
- eventType (Aktion)
- objectId (documentId oder folderId)
- objectType (Dokument oder Ordner)
- softwareModule (in welchem Modul die Änderungen vorgenommen werden)
- tenantId (Kunde)
- transactionId (dient zur Gruppierung mehrerer Ereignisse, die mit einer Benutzeraktion durchgeführt werden)
- Benutzer (E-Mail)

Auf der Benutzeroberfläche sieht der Benutzer alle Änderungen, die an dem Dokument vorgenommen wurden, wann sie vorgenommen wurden und wer sie vorgenommen hat.

5.1. Allgemeine Aufzeichnungen

5.1.1. Zugriff eArchiv

Jeder Zugriff auf das eArchiv wird aufgezeichnet.

5.2. Aufzeichnungen Dokumente

Alle Änderungen an Dokumentinformationen (Metadaten) und Zugriffe auf Dokumente werden aufgezeichnet und gespeichert. Die Aufzeichnungen erfolgen innerhalb von KLARA und werden schlussendlich täglich am Tagesende auf Google Cloud Storage als .csv File gespeichert.

5.2.1. Dokumentenzugriff

Jeder Zugriff auf ein Dokument wird aufgezeichnet.

5.2.2. Dokumenterhalt

Erhält der Kunde ein Dokument zugestellt, wird dessen erhalt aufgezeichnet. Wird ein Dokument bereits mit einem vordefinierten Dokumenttyp eingeliefert, so wird dieser entsprechend in der Aufzeichnung erwähnt.

5.2.3. Dokumentupload

Lädt ein User ein Dokument manuell ins Archiv, wird dessen Upload aufgezeichnet. Wird das Dokument direkt in einen bestehenden Archivordner heraufgeladen, so wird dieser entsprechend in der Aufzeichnung erwähnt.

5.2.4. Dokumentverarbeitung

Nachdem dem Kunde ein Dokument zugestellt wurde, wird dieses durch KLARA entsprechend verarbeitet und mit zusätzlichen Informationen angereichert. Bei dieser Verarbeitung wird das Dokument unter Anderem signiert und der Dokumenttyp wird ausgelesen (sofern nicht bereits durch Dritte definiert). Die Signatur sowie die Definition des Dokumenttypes werden aufgezeichnet.

5.2.5. Nachträglicher Fileupload

Innerhalb von KLARA kann ein Dokument nur aus Dokumentinformationen bestehen und kein Referenzfile besitzen. Das Referenzfile kann jedoch nachträglich zu den Dokumentinformationen hinzugefügt werden. Dieser nachträgliche Fileupload wird aufgezeichnet.

5.2.6. SmartLetter

Als spezielle Briefform bietet KLARA ihren Kunden einen sogenannten «SmartLetter» an. Dieser kann lediglich digital zugestellt werden und bietet dem Empfänger die Möglichkeit eine Antwort als Reaktion auf den Inhalt zu senden. Der «SmartLetter» wird als PDF/A innerhalb von KLARA gespeichert und, wie ein ordentliches Dokument, signiert und mit einem Zeitstempel versehen. Der Erhalt dieser speziellen Briefform sowie der Zeitpunkt der Antwort durch den Empfänger werden aufgezeichnet.

5.2.7. Dokumentarchivierung

Wird ein Dokument durch einen User archiviert, wird dies aufgezeichnet. Dabei wird die Referenz zum Ordner, in welchem das Dokument gespeichert wurde, in der Aufzeichnung erwähnt.

5.2.8. Dokumentenänderungen

Jegliche Änderung an Dokumentinformationen (Metadaten) werden aufgezeichnet. Dazu gehören Änderungen an:

- Titel
- Beschreibung
- Dokumenttyp
- Betrag (bei Rechnungen)
- Fälligkeitsdatum (bei Rechnungen)
- Tags

Werden Änderungen am Dokumenttyp oder den Tags vorgenommen, werden diese entsprechend in der Aufzeichnung erwähnt.

5.2.9. Dokumentverschiebung

Ein Dokument kann innerhalb des Archives von einem Ordner in einen anderen Ordner verschoben werden. Zusätzlich besteht die Möglichkeit, dass ein Dokument kopiert und in einem zusätzlichen Ordner abgelegt werden kann. Die Verschiebung sowie das Kopieren eines Dokuments werden aufgezeichnet. Bei beiden Operationen wird die Referenz zum Ordner, in welchem das Dokument kopiert / verschoben wurde oder von Ordner, aus welchem das Dokument verschoben wurde, in der Aufzeichnung erwähnt.

5.2.10. Dokumentlöschung

Wird ein Dokument durch einen User gelöscht, wird dieses in einen Papierkorb verschoben. Das Dokument ist für 30 Tage im Papierkorb sichtbar, bevor es durch das System endgültig gelöscht wird. Alternativ hat ein User jedoch die Möglichkeit, das Dokument ebenfalls manuell endgültig zu löschen. Die Verschiebung des Dokuments in den Papierkorb sowie die automatische oder manuelle endgültige Löschung des Dokumentes werden aufgezeichnet.

5.2.11. Dokumentwiederherstellung

Ein Dokument, welches in den Papierkorb verschoben wurde, kann durch einen User wiederhergestellt werden. Die Wiederherstellung wird entsprechend aufgezeichnet. Wird das Dokument in einen Ordner wiederhergestellt, so wird die Referenz zum Ordner, in welchem das Dokument wiederhergestellt wurde, in der Aufzeichnung erwähnt.

5.2.12. Aktionen annullieren

Bestimmte Dokumentaktionen können durch den User annulliert werden. Dazu gehören:

- Archivierung
- Löschung
- Kopie
- Verschiebung

Wird eine Aktion annulliert, wird diese aufgezeichnet. Bei der Annullierung der Archivierung und Kopie eines Dokumentes wird die Referenz zum Ordner, in welches das Dokument ursprünglich archiviert / kopiert werden sollte, in der Aufzeichnung erwähnt.

5.3. Aufzeichnungen Ordner

Alle Änderungen an Ordnerinformationen (Metadaten) und Zugriffe auf Ordner werden aufgezeichnet und gespeichert. Die Aufzeichnungen erfolgen innerhalb von KLARA und werden schlussendlich auf Google Cloud Storage als .csv File gespeichert.

5.3.1. Ordnerstellung

Wird ein Ordner im Archiv durch einen User erstellt, wird die Erstellung aufgezeichnet. Bei der Erstellung eines Unterordners wird zusätzlich die Referenz zum übergeordneten Ordner in den Aufzeichnungen erwähnt.

5.3.2. Ordnerzugriff

Jeder Zugriff auf einen Ordner durch einen User wird aufgezeichnet.

5.3.3. Ordnerverschiebung

Ein Ordner kann innerhalb des Archives von Root Folder in einen Ordner oder von einem Ordner in einen anderen Ordner verschoben werden. Dabei wird die Referenz zum übergeordneten Ordner in den Aufzeichnungen erwähnt, in welchem der Ordner verschoben oder aus welchem der Ordner verschoben wurde.

5.3.4. Namensänderung

Änderung am Namen des Ordners werden aufgezeichnet.

5.3.5. Ordnerlöschung

Wird ein Ordner durch einen User gelöscht, wird dieser mitsamt aller in ihm gespeicherten Dokumente in einen Papierkorb verschoben. Der Ordner und dessen Inhalt ist für 30 Tage im Papierkorb sichtbar, bevor er durch das System endgültig gelöscht wird. Alternativ hat ein User jedoch die Möglichkeit, den Ordner und / oder dessen Inhalt ebenfalls manuell endgültig zu löschen. Die Verschiebung des Ordners in den Papierkorb sowie die automatische oder manuelle endgültige Löschung des Ordners werden aufgezeichnet.

Ausnahme: Wird ein Dokument in mehrere Ordner gespeichert und dann einer dieser Ordner gelöscht, so wird das Dokument nicht in den Papierkorb verschoben.

5.3.6. Ordnerwiederherstellung

Ein Ordner, welcher in den Papierkorb verschoben wurde, kann durch einen User wiederhergestellt werden. Die Wiederherstellung wird entsprechend aufgezeichnet. Wird der Ordner in einen anderen Ordner wiederhergestellt, so wird die Referenz zum Ordner, in welchem der Ordner wiederhergestellt wurde, in der Aufzeichnung erwähnt.

6. Integrität von Dokumenten und Aufzeichnungen

6.1. Einsatz digitaler Signaturen

KLARA verwendet bei Dokumenten und Aufzeichnen digitale Signaturen und Zeitstempel, um die Beweiskraft der archivierten Dokumente und deren Logs zu erhöhen. Dokumenten und Aufzeichnungen werden bei der Erstellung mit einer digitalen Signatur versehen. Somit erhalten alle Dokumente und Aufzeichnungen innerhalb von «eArchiv» einen Zeitstempel.

Digitale Signaturen werden durch externe offizielle Anbieter erzeugt und als separate Signaturdatei dem eigentlichen Dokument zugeordnet, indem es am gleichen Speicherort abgespeichert wird. Als externe offizielle Anbieter werden «Swiss TSA», betrieben durch das BIT und «FreeTSA.org» eingesetzt. Dabei wird «Swiss TSA» per Default verwendet und «FreeTSA.org» als Backup, falls «Swiss TSA» nicht verfügbar ist.

Am Ende des Tages werden alle Aufzeichnungen pro Kunde in eine .csv-Datei exportiert. Es wird ein Hash der Datei generiert und die Datei selbst wird pro Kunde auf Google Cloud Storage gespeichert. Die Hashes aller exportierten Dateien werden in einer weiteren Datei zusammengeführt. Diese neu generierte Datei wird mit einem Zeitstempel versehen und systemspezifisch auf Google Cloud Storage gespeichert.

6.1.1. Integrity Check

KLARA prüft die Gültigkeit der Signatur bei jedem User Login (max. 1x pro Tag) und vergleicht dabei ebenfalls den Hash der Anfrage mit einem neu generierten Hash des Dokumentes. Ein Dokument ist nur integer, wenn die Signatur gültig ist und die beiden Hashes übereinstimmen.

Falls die Hashes nicht übereinstimmen oder die Signatur nicht mehr gültig ist, wird eine interne Alarmierung erstellt und die KLARA Business AG prüft, was die Ursache für die Nichtübereinstimmung ist und korrigiert sie.

Mit dieser Integritätsprüfung werden folgenden Tests durchgeführt:

1. Prüfung, ob die Dokumente entschlüsselt werden können
2. Prüfung, ob jedes Dokument eine digitale Signatur hat
3. Überprüfung der Übereinstimmung der digitalen Signaturen

6.2. Einsatz Blockchain Technologie

Um die Integrität jeder einzelnen Aufzeichnung zu gewährleisten, wird ein Hash von allen Daten der aktuellen Aufzeichnungen und dem Hash der vorherigen Aufzeichnungen berechnet. Damit werden die einzelnen Aufzeichnungen miteinander zu einer "Kette" verknüpft. Dieser Prozess wird über den Tag verteilt durchgeführt, sobald eine Aufzeichnung generiert wird.

Täglich werden alle Hashes rekalkuliert und mit den originalen Hashes verglichen. Die Aufzeichnungen sind nur integer, wenn die rekalkulierten Hashes mit den originalen Hashes übereinstimmen. Nachfolgeprozesse werden erst gestartet, wenn die Integrität der Aufzeichnungen gewährleistet werden kann.

Falls die Hashes nicht übereinstimmen, werden alle Prozesse rund um die Aufzeichnungen von «eArchiv» gestoppt und eine interne Alarmierung (davon ausgeschlossen ist die Erstellung der Aufzeichnungen). Die KLARA Business AG prüft dann, was die Ursache für die Nichtübereinstimmung ist und korrigiert sie. Erst nach der Korrektur werden die Nachfolgeprozesse wieder gestartet.

Im Störungsfall führt KLARA ein Fehlerprotokoll und speichert dieses innerhalb von «eArchiv» ab.

7. Generelle Bemerkungen

Der Betrieb von «eArchiv» erfolgt auf der Goolge Cloud Plattform (GCP) und alle Daten werden auf Google Cloud Storage gespeichert.

Die Zertifizierungen der Google Cloud Plattform können hier eingesehen werden.

Die KLARA Business AG ist ein nach ISO27001 zertifiziertes Unternehmen.