KLARA
Simplifies your business.

GEBÜV-COMPLIANT ARCHIVING WITH KLARA eARCHIVE

Documentation for Customers

Version 1.0, February 2023

Table of Contents

1. Introduction

This document serves as a manual for the GeBüV-compliant operation of the electronic archive with the product «eArchive» by KLARA Business AG.

This document is not a user manual for the «eArchive» product but rather outlines the GeBüV-compliant procedures. Additionally, it presents organizational guidelines and recommendations that should be considered for GeBüV-compliant use.

1.1. KLARA and eArchive

Payroll accounting, employee insurance, work certificates, illness and accident reports, or accounting take up a lot of time and energy from small business owners and private households alike. Valuable time that could be better spent on daily business or leisure activities. KLARA has addressed this issue and found an innovative solution: KLARA takes on much more than just administrative tasks, making office work simple. Furthermore, KLARA is a certified Google Partner.

Paid additional offerings underscore this core service and help customers run their business more productively. One such paid additional offering is «eArchive».

The KLARA eArchive product enables KLARA's customers to digitally archive documents in compliance with GeBüV. At a minimum, the «Basic» version must be used for GeBüV-compliant deployment. Optionally, the «Plus» version can be subscribed to, which includes additional access management to manage permissions at the document or folder level.

1.2. GeBüV

The Ordinance on the Keeping and Retention of Business Records (GeBüV) of April 2002 (as of January 1, 2013) is based on Article 958f Paragraph 4 of the Swiss Code of Obligations. The GeBüV specifies the books to be maintained and sets out general principles for the keeping and retention of records. It also provides principles for proper storage in particular and information on permissible data carriers and procedures. GeBüV is divided into five sections:

1. Books to be maintained – main ledger and, depending on the type and scope of the business, also subsidiary ledgers
2. General principles for the proper keeping and retention of books, integrity, documentation.
3. Principles for proper storage – due diligence, availability, organization, archive
4. Data carriers – permissible data carriers, verification, and data migration
5. Final provisions - entry into force and repeal of previous law

Documentation on GeBüV is available online via the following link: https://www.admin.ch/opc/de/classified-compilation/20001467/index.html

2. eArchive Operational Recommendations

The following are organizational recommendations to be observed when using «eArchive». These requirements can be mapped within the KLARA core offering.

2.1. Archive Formats

The KLARA eArchive can store and archive a variety of formats. For long-term archiving and archiving in compliance with GeBüV, it is important to use long-term archive formats. The KLARA eArchive guarantees GeBüV-compliant archiving exclusively with the format «PDF/A» and therefore converts all PDF files into PDF/A.

2.2. Authentication and Authorization

The assignment and management of general access permissions can only be performed within KLARA. For the assignment and management of access permissions at the document or folder level, the «eArchive» offering in the «Plus» variant is required.

Identity management of users can only be conducted outside of KLARA by the customer. Accordingly, the customer is responsible for the appropriate organization and documentation or can refer to relevant guidelines and documentation.

Furthermore, it is essential to ensure that all natural persons who use KLARA as users of a company receive their own, personal user profile and are recorded as users of a company within the KLARA core offering. Otherwise, it is not guaranteed that anonymous access is prevented.

The customer is responsible for organizing, documenting, and managing access permissions, particularly for revoking access rights when an employee leaves the company.

All relevant passwords to administrative user profiles (Users) for accessing KLARA and managing within KLARA must be managed by the customers through a documented procedure. The use of user profiles or passwords, particularly for critical information access, should be organized according to the four-eyes principle. This is especially true for resetting passwords.

The assignment of administrative user profiles (Users) must be regularly checked within the KLARA core offering by the customer and adjusted if necessary.

Every user of KLARA who needs to access documents archived in accordance with GeBüV (or the system itself) must be registered within the KLARA core offering. KLARA does not recognize anonymous users.

2.3. Retention Periods

The periods for retaining archive documents according to GeBüV must be determined by the customer. Note that additional regulatory or legal requirements may result in periods that exceed the requirements of GeBüV. Compliance with these periods is the responsibility of the customer and is not regulated/checked by «eArchive».

Possible laws affecting retention periods include:

- Data Protection Law
- Law on the second pillar of pension funds
- etc.

2.4. Integrity Verification

The customer is obligated to verify the integrity of a file uploaded from an external source before it is archived. KLARA performs an integrity check at each user login (once per day maximum) in the eArchive, which proceeds as follows:

- Verification of the validity of document signatures by comparing hashes of the request with a newly generated hash of the document for 100 documents
- Checking whether the documents can be decrypted
- Checking whether each document has a digital signature
- Verification of the consistency of digital signatures
- If an error occurs during this verification, an internal alarm is triggered to identify and address the problem cause
- Subsequently, the hashes of the affected documents are recalculated to ensure the signature

2.5. Exporting Documents

When exporting documents from the archive, KLARA provides the original formats, electronic signatures, and the log files.

The exported data is available to the customer via a personal download link for 14 days and can only be decrypted using a password previously defined by an administrative user profile.

In the event of an export of archive data, KLARA recommends checking the downloaded documents for completeness and correctness.

3. Technical Features

3.1. Data Storage

All documents in original formats (PDF/A), further documents and document information, and log files are stored by KLARA in Google Cloud Storage in Switzerland with multiple redundancies. The documents in original formats are encrypted customer-specific to protect against unauthorized insights and alterations.

The data backup is conducted using the usual backup procedures, which KLARA Business AG already employs.

3.2. Backups

Data backup is performed in several ways:

Snapshots
- A daily snapshot of the data carrier of the database is created. These snapshots have a lifespan of 14 days.

Standby Database
- WAL files from the main database are stored in the WAL storage.
- A secondary standby database reads the WAL files from the WAL storage and is thus kept up to date.

Full Backups on Backup Server
- Weekly full backups are made from the standby database and delivered to the backup server. The WAL files are synchronized from the WAL storage to the backup server.

Backup Security
- All WAL and backup files are also synchronized with a GCP Storage Bucket located in a separate GCP project.

3.3. Restoration

Depending on the issue KLARA is facing, the following restoration procedures occur:

The data (hard drive) of the main database is damaged.

- The data of the standby database server is duplicated and used for the main database.

The data (data carriers) of both the main and the standby databases are damaged.

- The last snapshot of the main database's disk is used as the starting point.
- All WALs generated since this snapshot are applied.
- The resulting data disk is duplicated and used for the standby server.

The data (hard drive) of both the main and standby databases are damaged, and all snapshots are also damaged.

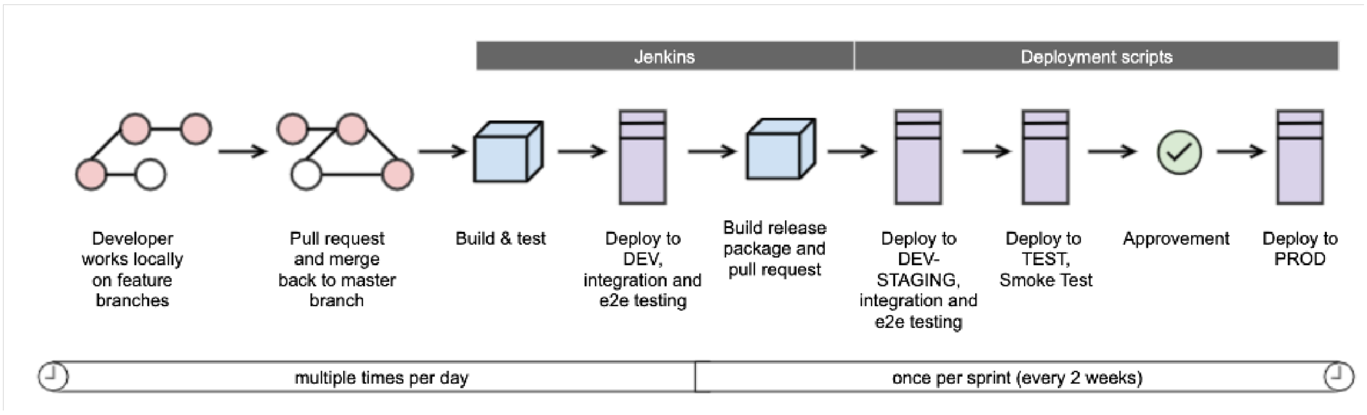
- The last full backup of the database is taken as the starting point.
- All WALs created since this backup are applied.
- The resulting data disk is duplicated and used for the standby server.

All data in the GCP project is damaged.

- Main and standby database servers are set up anew.
- The last full backup of the database in a separate GCP project is taken as the starting point. All WALs generated since this backup are taken over from the separate GCP project.

3.4. Change Process

Before a new version of software is deployed at KLARA, it undergoes several test phases to ensure backward compatibility and error-free operation. The following diagram outlines the procedure at KLARA:


Jenkins
Deployment scripts
Developer works locally on feature branches
Pull request and merge back to master branch
Build & test
Deploy to DEV, integration and e2e testing
Build release package and pull request
Deploy to DEV-STAGING, integration and e2e testing
Deploy to TEST, Smoke Test
Approvement
Deploy to PROD
multiple times per day
once per sprint (every 2 weeks)

4. Variants

4.1. Basic

«eArchive» includes a range of features in the standard delivery «Basic» that enable a comprehensible operation of an electronic document archive that meets the usual requirements for legally compliant retention.

The features included in the standard scope of «eArchive» are as follows:

- All documents are stored in a tamper-proof (encrypted) manner and can only be viewed by the customer.
- All changes and accesses to documents (metadata) are recorded and stored.
- The changes are linked together using a blockchain procedure.
- All changes to the document are displayed to the user as history in the user interface.
- Each document is provided with an external signature, and information about this is displayed to the user on the user interface.
- Regular integrity checks as per the integrity verification.

4.2. Plus

The additional option «Plus» includes all features contained in the standard delivery «Basic». Additionally, this option provides the capability to define access rights at the document or folder level. This has been implemented as follows:

1. Each business object (document or folder) can be assigned one or more security classes.
2. Each user can be assigned one or more security classes.
3. A user has access to the business objects that correspond to at least one of the security classes assigned to them.
4. The administrator of the company profile in KLARA Business always has access to all documents.

5. Records

Changes to documents and folders are tracked by creating events that document changes to the metadata of the document or folder. The following metadata changes are tracked and specifically mentioned in the event (values are encrypted):

- Changes to the document type
- Änderungen an der Ordnerverknüpfung eines Dokuments
- Changes to tags

An event consists of the following data:

- Id (unique ID)
- auditData (changes to document type, folder linkage, or tags)
- eventDateTime (timestamp)
- eventDescription (user action)
- eventFingerprint (calculated hash value)
- eventStatus (successful or failed)
- eventSubType (object; document, file, metadata, etc.)
- eventType (action)
- objectId (documentId or folderId)
- objectType (document or folder)
- softwareModule (in which module the changes were made)
- tenantId (customer)
- transactionId (used to group multiple events that are performed with a user action)
- User (email)

On the user interface, the user sees all changes made to the document, when they were made, and who made them.

5.1. General Records

5.1.1. eArchive Access

Every access to the eArchive is recorded.

5.2. Document Records

All changes to document information (metadata) and accesses to documents are recorded and stored. The records are made within KLARA and are ultimately stored daily at the end of the day on Google Cloud Storage as a .csv file.

5.2.1. Document Access

Every access to a document is recorded.

5.2.2. Document Receipt

When a customer receives a document, its receipt is recorded. If a document is delivered with a predefined document type, it is mentioned accordingly in the record.

5.2.3. Document Upload

When a user manually uploads a document into the archive, this upload is recorded. If the document is uploaded directly into an existing archive folder, this is mentioned accordingly in the record.

5.2.4. Document Processing

After a document is delivered to the customer, it is processed by KLARA and enriched with additional information. During this processing, the document is, among other things, signed and the document type is read (unless already defined by a third party). The signature and the definition of the document type are recorded.

5.2.5. Subsequent File Upload

Within KLARA, a document may consist only of document information and have no reference file. However, the reference file may be added to the document information subsequently. This subsequent file upload is recorded.

5.2.6. SmartLetter

As a special form of letter, KLARA offers its customers a so-called «SmartLetter» which can only be delivered digitally and provides the recipient with the opportunity to send a response reacting to the content. The «SmartLetter» is stored within KLARA as a PDF/A and, like a proper document, is signed and timestamped. The receipt of this special form of letter and the time of response by the recipient are recorded.

5.2.7. Document Archiving

When a document is archived by a user, this is recorded. The reference to the folder in which the document was stored is mentioned in the record.

5.2.8. Document Changes

Any changes to document information (metadata) are recorded. These include changes to:

- Title
- Description
- Document type
- Amount (for invoices)
- Due date (for invoices)
- Tags

Changes to the document type or tags, if made, are mentioned accordingly in the record.

5.2.9. Document Movement

A document can be moved within the archive from one folder to another folder. Additionally, a document can be copied and placed in an additional folder. Both the movement and the copying of a document are recorded. In both operations, the reference to the folder in which the document was copied/moved or from which folder the document was moved, is mentioned in the record.

5.2.10. Document Deletion

When a document is deleted by a user, it is moved to the trash. The document remains visible in the trash for 30 days before it is permanently deleted by the system. Alternatively, a user has the option to also manually delete the document permanently. The movement of the document to the trash as well as the automatic or manual final deletion of the document are recorded.

5.2.11. Document Restoration

A document that has been moved to the trash can be restored by a user. The restoration is recorded accordingly. If the document is restored to a folder, the reference to the folder in which the document was restored is mentioned in the record.

5.2.12. Canceling Actions

Certain document actions can be canceled by the user. These include:

- Archiving
- Deletion
- Copying
- Movement

When an action is canceled, this is recorded. In the cancellation of the archiving and copying of a document, the reference to the folder into which the document was originally to be archived/copied is mentioned in the record.

5.3. Folder Records

All changes to folder information (metadata) and accesses to folders are recorded and stored. The records are made within KLARA and are ultimately stored on Google Cloud Storage as a .csv file.

5.3.1. Folder Creation

When a user creates a folder in the archive, the creation is recorded. In the case of creating a subfolder, the reference to the parent folder is additionally mentioned in the records.

5.3.2. Folder Access

Every access to a folder by a user is recorded.

5.3.3. Folder Movement

A folder can be moved within the archive from the root folder to another folder, or from one folder to another folder. In doing so, the reference to the parent folder is mentioned in the records, where the folder was moved to or from which the folder was moved.

5.3.4. Name Change

Changes to the name of the folder are recorded.

5.3.5. Folder Deletion

When a folder is deleted by a user, it and all documents stored within it are moved to the trash. The folder and its contents are visible in the trash for 30 days before being permanently deleted by the system. Alternatively, a user can also manually delete the folder and/or its contents permanently. The movement of the folder to the trash as well as the automatic or manual final deletion of the folder are recorded.

Exception: If a document is stored in multiple folders and then one of these folders is deleted, the document is not moved to the trash.

5.3.6. Folder Restoration

A folder that has been moved to the trash can be restored by a user. The restoration is recorded accordingly. If the folder is restored to another folder, the reference to the folder in which the folder was restored is mentioned in the record.

6. Integrity of Documents and Records

6.1. Use of Digital Signatures

KLARA uses digital signatures and timestamps on documents and records to increase the evidentiary value of the archived documents and their logs. Documents and records are provided with a digital signature upon creation. Thus, all documents and records within «eArchive» are timestamped.

Digital signatures are generated by external official providers and are stored as a separate signature file at the same storage location as the actual document. The external official providers used are «Swiss TSA», operated by the BIT, and «FreeTSA.org» as a backup if «Swiss TSA» is unavailable. «Swiss TSA» is used by default.

At the end of the day, all records per customer are exported into a .csv file. A hash of the file is generated, and the file itself is stored per customer on Google Cloud Storage. The hashes of all exported files are merged into another file. This newly generated file is timestamped and stored system-specifically on Google Cloud Storage.

6.1.1. Integrity Check

KLARA checks the validity of the signature at each user login (maximum once per day) and compares the hash of the request with a newly generated hash of the document. A document is only considered intact if the signature is valid and both hashes match.

If the hashes do not match or the signature is no longer valid, an internal alarm is triggered, and KLARA Business AG investigates the cause of the mismatch and corrects it.

This integrity check includes the following tests:

1. Checking whether the documents can be decrypted.
2. Checking whether each document has a digital signature.
3. Verification of the consistency of digital signatures.

6.2. Use of Blockchain Technology

To ensure the integrity of each individual record, a hash is calculated from all the data of the current records and the hash of the previous records. Thus, the individual records are linked together to form a «chain». This process is performed throughout the day, as soon as a record is generated.

Every day, all hashes are recalculated and compared with the original hashes. The records are only considered intact if the recalculated hashes match the original hashes. Subsequent processes are only started if the integrity of the records can be guaranteed.

If the hashes do not match, all processes related to the records of «eArchive» are stopped, and an internal alarm is triggered (excluding the creation of the records). KLARA Business AG then investigates the cause of the mismatch and corrects it. Only after the correction are the subsequent processes restarted.

In the event of a disruption, KLARA maintains an error log and stores it within «eArchive».

7. General Remarks

The operation of «eArchive» is carried out on the Google Cloud Platform (GCP), and all data is stored on Google Cloud Storage.

The certifications of the Google Cloud Platform can be viewed here.

KLARA Business AG is a company certified according to ISO27001.

Zertifiziertes Managementsystem
SQS
ISO/IEC 27001