



**KLARA**

Simplifie tes tâches de bureau.

# **ARCHIVAGE CONFORME À GEBÜV AVEC KLARA eARCHIVE**

## Documentation pour clients

Version 1.0, Février 2023

# Table des matières

<b>1. INTRODUCTION .....</b>	<b>4</b>
1.1. KLARA ET EARCHIV .....	4
1.2. GEBÜV .....	4
<b>2. RECOMMANDATIONS OPÉRATIONNELLES DE EARCHIV .....</b>	<b>5</b>
2.1. FORMATS D'ARCHIVE .....	5
2.2. AUTHENTIFICATION ET AUTORISATION .....	5
2.3. DURÉES DE CONSERVATION .....	5
2.4. VÉRIFICATION DE L'INTÉGRITÉ.....	6
2.5. EXPORTATION DE DOCUMENTS .....	6
<b>3. CARACTÉRISTIQUES TECHNIQUES .....</b>	<b>6</b>
3.1. MAINTENANCE DES DONNÉES .....	6
3.2. SAUVEGARDES .....	6
3.3. RESTAURATION .....	7
3.4. PROCESSUS DE CHANGEMENT .....	7
<b>4. VARIANTES .....</b>	<b>8</b>
4.1. BASIC .....	8
4.2. PLUS .....	8
<b>5. ENREGISTREMENTS .....</b>	<b>9</b>
<b>5.1. ENREGISTREMENTS GÉNÉRAUX .....</b>	<b>9</b>
5.1.1. ACCÈS EARCHIV .....	9
<b>5.2. ENREGISTREMENTS DES DOCUMENTS .....</b>	<b>9</b>
5.2.1. ACCÈS AUX DOCUMENTS.....	9
5.2.2. CONSERVATION DES DOCUMENTS .....	9
5.2.3. TÉLÉVERSEMENT DE DOCUMENTS .....	9
5.2.4. TRAITEMENT DES DOCUMENTS .....	10
5.2.5. TÉLÉVERSEMENT DE FICHER ULTÉRIEUR .....	10
5.2.6. SMARTLETTER .....	10
5.2.7. ARCHIVAGE DES DOCUMENTS .....	10
5.2.8. MODIFICATIONS DES DOCUMENTS .....	10
5.2.9. DÉPLACEMENT DES DOCUMENTS .....	10
5.2.10. SUPPRESSION DES DOCUMENTS .....	10
5.2.11. RESTAURATION DES DOCUMENTS .....	11
5.2.12. ANNULATION D'ACTIONS .....	11
<b>5.3. ENREGISTREMENTS DES DOSSIERS.....</b>	<b>11</b>
5.3.1. CRÉATION DE DOSSIERS.....	11
5.3.2. ACCÈS AUX DOSSIERS .....	11

5.3.3. DÉPLACEMENT DES DOSSIERS .....	11
5.3.4. CHANGEMENT DE NOM .....	11
5.3.5. SUPPRESSION DES DOSSIERS.....	11
5.3.6. RESTAURATION DES DOSSIERS .....	12
<b>6. INTÉGRITÉ DES DOCUMENTS ET ENREGISTREMENTS .....</b>	<b>13</b>
<b>6.1. UTILISATION DES SIGNATURES NUMÉRIQUES .....</b>	<b>13</b>
6.1.1. CONTRÔLE D'INTÉGRITÉ .....	13
<b>6.2. UTILISATION DE LA TECHNOLOGIE BLOCKCHAIN .....</b>	<b>13</b>
<b>7. REMARQUES GÉNÉRALES .....</b>	<b>14</b>

## 1. Introduction

Ce document sert de manuel pour l'opération conforme à GeBüV de l'archive électronique avec le produit « eArchiv » de KLARA Business AG.

Ce document n'est pas un mode d'emploi pour le produit « eArchiv », mais il énumère uniquement les procédures conformes à GeBüV. De plus, des directives organisationnelles et des recommandations sont présentées, qui doivent être prises en compte ou sont nécessaires pour une utilisation conforme à GeBüV.

### 1.1. KLARA et eArchiv

Les fiches de paie, les assurances des employés, les certificats de travail, les notifications de maladie et d'accident ou la comptabilité prennent beaucoup de temps et d'efforts aux petits entrepreneurs ainsi qu'aux ménages privés. Du temps précieux que l'on préférerait investir dans les affaires quotidiennes ou les loisirs. KLARA a examiné ce problème et a trouvé une solution innovante : KLARA prend en charge bien plus que le simple fardeau administratif, rendant ainsi le bureau simple. De plus, KLARA est un partenaire certifié Google.

Les offres supplémentaires payantes soulignent cette offre principale et aident les clients à rendre leur activité encore plus productive. L'une de ces offres supplémentaires payantes est « eArchiv ».

Le produit KLARA eArchiv permet aux clients de KLARA une archivage numérique conforme à GeBüV. Pour une utilisation conforme à GeBüV de « eArchiv », il est nécessaire d'utiliser au moins la variante « Basic ». Il est possible de souscrire à la variante « Plus », qui dispose d'une gestion d'accès supplémentaire, permettant de gérer les autorisations au niveau des documents ou des dossiers.

### 1.2. GeBüV

L'ordonnance sur la tenue et la conservation des livres de commerce (GeBüV) d'avril 2002 (version du 1er janvier 2013) est basée sur l'article 958f alinéa 4 du Code des obligations suisse. La GeBüV spécifie les livres à tenir et établit des principes généraux pour la tenue et la conservation des livres. En outre, elle définit les principes pour une conservation appropriée en particulier, ainsi que des informations sur les supports d'information admissibles et les procédures. GeBüV est divisée en cinq sections :

1. Livres à tenir – grand livre et, selon la nature et l'étendue des affaires, aussi des livres auxiliaires
2. Principes généraux de tenue et de conservation appropriées des livres, intégrité, documentation
3. Principes pour une conservation appropriée – diligence, disponibilité, organisation, archives
4. Supports d'information – Supports d'information admissibles, vérification et migration de données
5. Dispositions finales - Entrée en vigueur et abrogation du droit antérieur

La documentation sur GeBüV est disponible sur Internet via le lien suivant :

<https://www.fedlex.admin.ch/eli/cc/2002/216/fr>

## 2. Recommandations opérationnelles de eArchiv

Les recommandations opérationnelles suivantes sont enregistrées, qui doivent être observées lors de l'utilisation de « eArchiv ». Ces exigences peuvent être représentées dans l'offre principale de KLARA.

### 2.1. Formats d'archive

Le KLARA eArchiv peut stocker et archiver une variété de formats différents. Pour l'archivage à long terme et l'archivage conforme à GeBüV, il est important d'utiliser des formats d'archives à long terme. Le KLARA eArchiv garantit l'archivage conforme à GeBüV exclusivement avec le format « PDF/a » et convertit donc tous les fichiers PDF en PDF/a.

### 2.2. Authentification et autorisation

L'attribution et la gestion des autorisations d'accès générales peuvent uniquement être effectuées au sein de KLARA. Pour l'attribution et la gestion des autorisations d'accès au niveau des documents ou des dossiers, l'offre « eArchiv » dans la variante « Plus » est nécessaire.

La gestion de l'identité des utilisateurs peut uniquement être effectuée par le client en dehors de KLARA. À cet égard, le client est responsable de l'organisation et de la documentation appropriées, ou peut se référer aux directives et documentations correspondantes.

De plus, il convient de veiller à ce que toutes les personnes physiques utilisant KLARA en tant qu'utilisateur d'une entreprise reçoivent un profil utilisateur personnel et soient enregistrées comme telles dans l'offre principale de KLARA. Autrement, l'accès anonyme n'est pas garanti.

Le client est responsable de l'organisation, de la documentation et de la gestion des autorisations d'accès, notamment pour la révocation des droits d'accès lors du départ d'un employé.

Tous les mots de passe pertinents des profils d'utilisateur administratifs (utilisateur) pour l'accès à KLARA et la gestion au sein de KLARA doivent être gérés par les clients via une procédure documentée. L'utilisation des profils d'utilisateur ou des mots de passe, dans la mesure où il s'agit d'accès à des informations critiques, doit être organisée selon le principe des quatre yeux. Cela s'applique également à la réinitialisation des mots de passe.

L'attribution des profils d'utilisateur administratifs (utilisateur) doit être régulièrement contrôlée par le client au sein de l'offre principale de KLARA et ajustée si nécessaire.

Chaque utilisateur de KLARA qui doit pouvoir accéder aux documents archivés conformément à GeBüV (ou au système lui-même) doit obligatoirement être enregistré dans l'offre principale de KLARA. KLARA ne reconnaît aucun utilisateur anonyme.

### 2.3. Durées de conservation

Les délais de conservation des documents d'archives selon GeBüV doivent être déterminés par le client. Il convient de noter que d'autres exigences réglementaires ou légales peuvent entraîner des délais qui vont au-delà des exigences de GeBüV (par exemple, la responsabilité du produit). Le respect des délais est de la responsabilité du client et n'est pas réglementé / vérifié par « eArchiv ».

Lois possibles ayant un impact sur les délais de conservation :

- Loi sur la protection des données
- Loi sur la deuxième colonne des fonds de pension
- etc.

## 2.4. Vérification de l'intégrité

Le client est tenu de vérifier l'intégrité d'un fichier provenant d'une source externe avant de l'archiver. KLARA effectue dans eArchiv une vérification de l'intégrité à chaque connexion de l'utilisateur (maximum une fois par jour), qui se déroule comme suit :

- Vérification de la validité de la signature des documents en comparant les hachages de la demande avec un hachage nouvellement généré du document sur 100 documents.
- Vérification de la capacité à déchiffrer les documents.
- Vérification de la présence d'une signature numérique sur chaque document.
- Contrôle de la correspondance des signatures numériques.
- En cas d'erreur lors de cette vérification, une alerte interne est déclenchée pour identifier la cause du problème et la corriger.
- Par la suite, les hachages des documents concernés sont recalculés pour garantir la signature.

## 2.5. Exportation de documents

KLARA fournit lors de l'exportation de documents de l'archive les formats originaux, les signatures électroniques, et les fichiers journaux.

Les données exportées sont mises à disposition du client pendant 14 jours via un lien de téléchargement personnel et ne peuvent être déchiffrées qu'avec un mot de passe défini auparavant par un profil d'utilisateur administratif (utilisateur).

En cas d'exportation des données d'archive, KLARA recommande de vérifier les documents téléchargés pour s'assurer de leur intégrité et de leur exactitude.

## 3. Caractéristiques techniques

### 3.1. Maintenance des données

Tous les documents au format original (PDF/A), d'autres documents et informations sur les documents ainsi que les fichiers journaux sont stockés par KLARA dans Google Cloud Storage en Suisse, de manière redondante multiple. Les documents au format original sont cryptés de manière spécifique au client, afin de les protéger contre les accès non autorisés et les modifications.

La sauvegarde des données est réalisée selon la procédure habituelle de sauvegarde que KLARA Business AG utilise déjà.

### 3.2. Sauvegardes

La sauvegarde des données est réalisée de plusieurs manières :

#### Snapshots

- Un instantané du disque de données de la base de données est créé quotidiennement. Ces instantanés ont une durée de vie de 14 jours.

#### Base de données en attente

- Les fichiers WAL de la base de données principale sont stockés dans le stockage WAL.
- Une base de données secondaire en attente lit les fichiers WAL du stockage WAL et est ainsi maintenue à jour.

#### Sauvegardes complètes sur serveur de sauvegarde

- Des sauvegardes complètes sont effectuées hebdomadairement à partir de la base de données en attente et envoyées au serveur de sauvegarde.
- Les fichiers WAL sont synchronisés du stockage WAL au serveur de sauvegarde.

### Sécurisation des sauvegardes

- Tous les fichiers WAL et de sauvegarde sont également synchronisés avec un GCP-Storage-Bucket, qui se trouve dans un projet GCP séparé.

### 3.3. Restauration

Selon le problème auquel KLARA est confrontée, les procédures de restauration suivantes sont effectuées :

Les données (disque) de la base de données principale sont endommagées.

- Les données du serveur de base de données en attente sont dupliquées et utilisées pour la base de données principale.

Les données (disques) de la base de données principale et de la base de données de réserve sont endommagées.

- Le dernier instantané du disque de la base de données principale est utilisé comme point de départ.
- Tous les WAL générés depuis cet instantané sont appliqués.
- Le disque de données résultant est dupliqué et utilisé pour le serveur en attente.

Les données (disque) de la base de données principale et en attente sont endommagées, et tous les instantanés sont également endommagés.

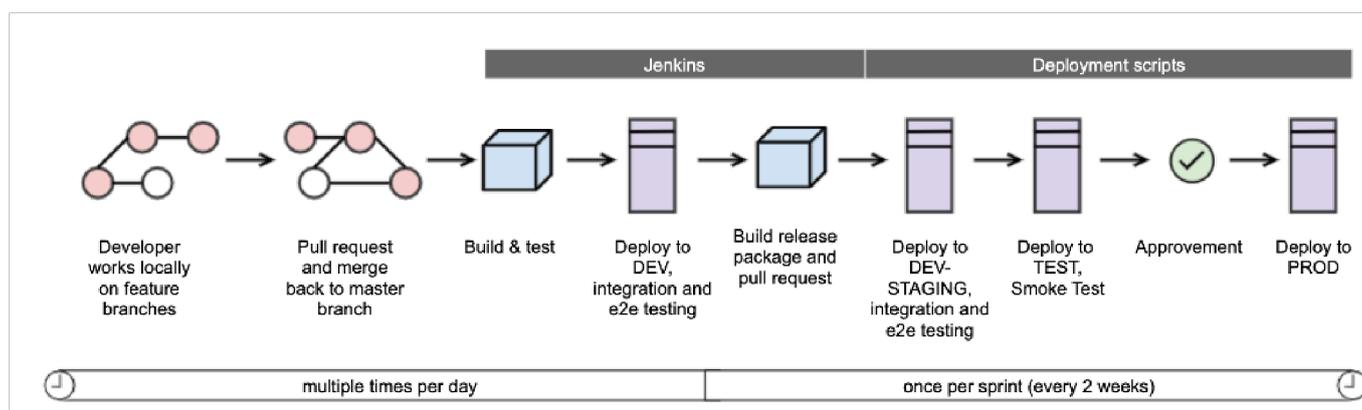
- La dernière sauvegarde complète de la base de données est prise comme point de départ.
- Tous les WAL créés depuis cette sauvegarde sont appliqués.
- Le disque de données résultant est dupliqué et utilisé pour le serveur en attente.

Toutes les données sur le projet GCP sont endommagées.

- Les serveurs de base de données principale et en attente sont reconstruits.
- La dernière sauvegarde complète de la base de données dans un projet GCP distinct est prise comme point de départ.
- Tous les WAL générés depuis cette sauvegarde sont pris du projet GCP séparé.

### 3.4. Processus de changement

Avant qu'une nouvelle version d'un logiciel soit mise en service chez KLARA, elle passe par plusieurs phases de test pour s'assurer qu'une compatibilité descendante et un fonctionnement sans erreur sont possibles. L'image suivante illustre la procédure chez KLARA :



## 4. Variantes

### 4.1. Basic

« eArchiv » dans sa livraison standard « Basic » comprend un ensemble de fonctionnalités qui permettent un fonctionnement conforme aux exigences légales habituelles de conservation des documents électroniques.

Les fonctionnalités incluses dans l'étendue standard de « eArchiv » comprennent les suivantes

- Tous les documents sont stockés de manière sécurisée (cryptés) et ne peuvent être consultés que par le client.
- Toutes les modifications et accès aux documents (métadonnées) sont enregistrés et stockés.
- Les modifications sont liées entre elles par une procédure de blockchain.
- Toutes les modifications apportées au document sont affichées à l'utilisateur comme historique dans l'interface utilisateur.
- Chaque document est doté d'une signature externe, et des informations à ce sujet sont affichées à l'utilisateur sur l'interface utilisateur.
- Vérification régulière de l'intégrité conformément à la vérification de l'intégrité.

### 4.2. Plus

L'option supplémentaire « Plus » comprend toutes les fonctionnalités contenues dans la livraison standard « Basic ». Cependant, cette option offre également la possibilité de définir des droits d'accès au niveau des documents ou des dossiers. Ceci a été mis en œuvre comme suit :

1. Chaque objet commercial (document ou dossier) peut se voir attribuer une ou plusieurs classes de sécurité.
2. Chaque utilisateur peut se voir attribuer une ou plusieurs classes de sécurité.
3. Un utilisateur a accès aux objets commerciaux qui correspondent au moins à une classe de sécurité qui lui a été attribuée.
4. L'administrateur du profil d'entreprise dans KLARA Business a toujours accès à tous les documents.

## 5. Enregistrements

Les modifications des documents et des dossiers sont suivies par la création d'événements qui documentent les modifications des métadonnées des documents ou des dossiers. Les modifications suivantes des métadonnées sont suivies et spécifiquement mentionnées dans les événements :

- Modifications du type de document
- Modifications de la liaison de dossier d'un document
- Modifications des tags

Un événement se compose des données suivantes :

- Id (identifiant unique)
- auditData (modifications du type de document, de la liaison de dossier ou des tags)
- eventDateTime (horodatage)
- eventDescription (action de l'utilisateur)
- eventFingerprint (empreinte hash calculée)
- eventStatus (réussi ou échoué)
- eventSubType (objet ; document, fichier, métadonnées, etc.)
- eventType (action)
- objectId (documentId ou folderId)
- objectType (document ou dossier)
- softwareModule (dans quel module les modifications ont été faites)
- tenantId (client)
- transactionId (utilisé pour regrouper plusieurs événements réalisés avec une action utilisateur)
- utilisateur (email)

Sur l'interface utilisateur, l'utilisateur voit toutes les modifications apportées au document, quand elles ont été faites et par qui.

### 5.1. Enregistrements généraux

#### 5.1.1. Accès eArchiv

Chaque accès à eArchiv est enregistré.

### 5.2. Enregistrements des documents

Toutes les modifications des informations sur les documents (métadonnées) et les accès aux documents sont enregistrés et stockés. Les enregistrements sont effectués au sein de KLARA et sont finalement stockés chaque jour en fin de journée sur Google Cloud Storage sous forme de fichier .csv.

#### 5.2.1. Accès aux documents

Chaque accès à un document est enregistré.

#### 5.2.2. Conservation des documents

Lorsque le client reçoit un document, sa réception est enregistrée. Si un document est livré avec un type de document prédéfini, ce type est mentionné dans l'enregistrement.

#### 5.2.3. Téléversement de documents

Lorsqu'un utilisateur téléverse manuellement un document dans l'archive, ce téléversement est enregistré. Si le document est téléversé directement dans un dossier d'archive existant, ce dossier est mentionné dans l'enregistrement.

#### 5.2.4. Traitement des documents

Après la livraison d'un document au client, celui-ci est traité par KLARA et enrichi d'informations supplémentaires. Pendant ce traitement, le document est, entre autres, signé et le type de document est extrait (s'il n'est pas déjà défini par des tiers). La signature et la définition du type de document sont enregistrées.

#### 5.2.5. Téléversement de fichier ultérieur

Au sein de KLARA, un document peut seulement consister en informations documentaires et ne pas posséder de fichier de référence. Le fichier de référence peut cependant être ajouté ultérieurement aux informations du document. Ce téléversement ultérieur de fichier est enregistré.

#### 5.2.6. SmartLetter

En tant que forme spéciale de lettre, KLARA offre à ses clients ce qu'on appelle un « SmartLetter ». Celui-ci peut uniquement être délivré de manière numérique et offre au destinataire la possibilité de répondre en réaction au contenu. Le « SmartLetter » est stocké chez KLARA en format PDF/A, comme un document ordinaire, signé et horodaté. La réception de cette forme spéciale de lettre ainsi que le moment de la réponse par le destinataire sont enregistrées.

#### 5.2.7. Archivage des documents

Lorsqu'un utilisateur archive un document, cela est enregistré. La référence au dossier dans lequel le document a été stocké est mentionnée dans l'enregistrement.

#### 5.2.8. Modifications des documents

Toute modification des informations sur les documents (métadonnées) est enregistrée. Cela inclut les modifications apportées à :

- Titre
- Description
- Type de document
- Montant (pour les factures)
- Date d'échéance (pour les factures)
- Tags

Lorsque des modifications sont apportées au type de document ou aux tags, celles-ci sont mentionnées dans l'enregistrement.

#### 5.2.9. Déplacement des documents

Un document peut être déplacé dans l'archive d'un dossier à un autre. De plus, il est possible que le document soit copié et déposé dans un dossier supplémentaire. Le déplacement ainsi que la copie d'un document sont enregistrés. Pour ces deux opérations, la référence au dossier dans lequel le document a été copié/déplacé, ou du dossier à partir duquel le document a été déplacé, est mentionnée dans l'enregistrement.

#### 5.2.10. Suppression des documents

Lorsqu'un utilisateur supprime un document, celui-ci est déplacé dans une corbeille. Le document reste visible pendant 30 jours dans la corbeille avant d'être définitivement supprimé par le système. Toutefois, un utilisateur peut également supprimer définitivement le document manuellement. Le déplacement du document dans la corbeille ainsi que la suppression automatique ou manuelle définitive du document sont enregistrés.

### 5.2.11. Restauration des documents

Un document déplacé dans la corbeille peut être restauré par un utilisateur. La restauration est enregistrée en conséquence. Si le document est restauré dans un dossier, la référence au dossier dans lequel le document a été restauré est mentionnée dans l'enregistrement.

### 5.2.12. Annulation d'actions

Certaines actions documentaires peuvent être annulées par l'utilisateur. Cela inclut :

- Archivage
- Suppression
- Copie
- Déplacement

Lorsqu'une action est annulée, cela est enregistré. Lors de l'annulation de l'archivage et de la copie d'un document, la référence au dossier dans lequel le document devait initialement être archivé/copié est mentionnée dans l'enregistrement.

## 5.3. Enregistrements des dossiers

Toutes les modifications des informations sur les dossiers (métadonnées) et les accès aux dossiers sont enregistrés et stockés. Les enregistrements sont effectués au sein de KLARA et sont finalement stockés sur Google Cloud Storage sous forme de fichier .csv.

### 5.3.1. Création de dossiers

Lorsqu'un dossier est créé dans l'archive par un utilisateur, la création est enregistrée. Lors de la création d'un sous-dossier, la référence au dossier parent est également mentionnée dans les enregistrements.

### 5.3.2. Accès aux dossiers

Chaque accès à un dossier par un utilisateur est enregistré.

### 5.3.3. Déplacement des dossiers

Un dossier peut être déplacé dans l'archive du dossier racine à un dossier ou d'un dossier à un autre dossier. La référence au dossier parent est mentionnée dans les enregistrements, dans lequel le dossier a été déplacé ou à partir duquel le dossier a été déplacé.

### 5.3.4. Changement de nom

Les modifications du nom du dossier sont enregistrées.

### 5.3.5. Suppression des dossiers

Lorsqu'un dossier est supprimé par un utilisateur, celui-ci, ainsi que tous les documents qu'il contient, sont déplacés dans une corbeille. Le dossier et son contenu restent visibles pendant 30 jours dans la corbeille avant d'être définitivement supprimés par le système. Toutefois, un utilisateur peut également supprimer définitivement le dossier et/ou son contenu manuellement. Le déplacement du dossier dans la corbeille ainsi que la suppression automatique ou manuelle définitive du dossier sont enregistrés.

Exception : Si un document est stocké dans plusieurs dossiers et qu'un de ces dossiers est supprimé, le document n'est pas déplacé dans la corbeille.

### 5.3.6. Restauration des dossiers

Un dossier déplacé dans la corbeille peut être restauré par un utilisateur. La restauration est enregistrée en conséquence. Si le dossier est restauré dans un autre dossier, la référence au dossier dans lequel le dossier a été restauré est mentionnée dans l'enregistrement.

## 6. Intégrité des documents et enregistrements

### 6.1. Utilisation des signatures numériques

KLARA utilise des signatures numériques et des horodatages pour augmenter la force probante des documents archivés et de leurs journaux. Les documents et enregistrements sont signés numériquement lors de leur création, ce qui garantit que tous les documents et enregistrements dans « eArchiv » reçoivent un horodatage.

Les signatures numériques sont générées par des fournisseurs officiels externes et sont associées en tant que fichier de signature séparé au document original, en étant stockées au même emplacement. Les fournisseurs officiels externes utilisés sont « Swiss TSA », géré par le BIT, et « FreeTSA.org ». « Swiss TSA » est utilisé par défaut et « FreeTSA.org » comme sauvegarde si « Swiss TSA » n'est pas disponible.

À la fin de la journée, tous les enregistrements par client sont exportés en un fichier .csv. Un hash du fichier est généré et le fichier lui-même est stocké sur Google Cloud Storage par client. Les hashes de tous les fichiers exportés sont regroupés dans un autre fichier. Ce nouveau fichier généré est horodaté et stocké spécifiquement sur Google Cloud Storage.

#### 6.1.1. Contrôle d'intégrité

KLARA vérifie la validité de la signature à chaque connexion de l'utilisateur (maximum une fois par jour) et compare également le hash de la demande avec un hash nouvellement généré du document. Un document est considéré comme intègre seulement si la signature est valide et si les deux hashes correspondent.

Si les hashes ne correspondent pas ou si la signature n'est plus valide, une alarme interne est déclenchée et KLARA Business AG examine la cause de la non-concordance et la corrige.

Avec cette vérification de l'intégrité, les tests suivants sont effectués :

1. Vérification de la capacité à déchiffrer les documents.
2. Vérification de la présence d'une signature numérique sur chaque document.
3. Vérification de la correspondance des signatures numériques.

### 6.2. Utilisation de la technologie Blockchain

Pour garantir l'intégrité de chaque enregistrement individuel, un hash est calculé à partir de toutes les données des enregistrements actuels et du hash des enregistrements précédents, reliant ainsi les enregistrements individuels en une « chaîne ». Ce processus est effectué tout au long de la journée dès qu'un enregistrement est généré.

Chaque jour, tous les hashes sont recalculés et comparés aux hashes originaux. Les enregistrements sont considérés comme intègres uniquement si les hashes recalculés correspondent aux hashes originaux. Les processus suivants ne sont démarrés que lorsque l'intégrité des enregistrements peut être garantie.

Si les hashes ne correspondent pas, tous les processus concernant les enregistrements de « eArchiv » sont arrêtés et une alarme interne est déclenchée (à l'exception de la création des enregistrements). KLARA Business AG examine alors la cause de la non-concordance et la corrige. Une fois la correction effectuée, les processus suivants sont redémarrés.

En cas de perturbation, KLARA tient un journal d'erreurs et le stocke dans « eArchiv ».

## 7. Remarques générales

L'exploitation de « eArchiv » se fait sur la plateforme Google Cloud (GCP) et toutes les données sont stockées sur Google Cloud Storage.

Les certifications de la plateforme Google Cloud peuvent être consultées [ici](#).

KLARA Business AG est une entreprise certifiée ISO 27001.

