KLARA
Semplifica i lavori d'ufficio.

ARCHIVIAZIONE CONFORME A GEBÜV CON KLARA

Documentazione per i client

Versione 1.0, Febbraio 2023

Indice dei contenuti

1. Introduzione

Questo documento serve come manuale per l'operatività conforme a GeBüV dell'archivio elettronico con il prodotto «eArchiv» di KLARA Business AG.

Questo documento non è un manuale d'uso per il prodotto «eArchiv», ma elenca solo le procedure conformi a GeBüV. Inoltre, vengono presentate le disposizioni organizzative e le raccomandazioni che dovrebbero essere prese in considerazione o sono necessarie per un impiego conforme a GeBüV.

1.1. KLARA e eArchiv

Buste paga, assicurazioni dei dipendenti, certificati di lavoro, notifiche di malattia e infortunio o contabilità tolgono molto tempo e nervi sia alle piccole imprese che alle famiglie. Tempo prezioso che si preferirebbe investire nell'attività quotidiana o nel tempo libero. KLARA ha affrontato questo problema e ha trovato una soluzione innovativa: KLARA allevia molto più che il semplice carico amministrativo, rendendo l'ufficio semplice. Inoltre, KLARA è un partner certificato Google.

Offerte aggiuntive a pagamento sottolineano questa offerta principale e aiutano i clienti a gestire l'attività in modo ancora più produttivo. Uno di questi servizi aggiuntivi a pagamento è «eArchiv».

Il prodotto KLARA eArchiv consente ai clienti di KLARA un'archiviazione digitale conforme a GeBüV. Per un impiego conforme a GeBüV di «eArchiv» è necessario almeno l'uso della variante «Basic». Facoltativamente, può essere sottoscritta la variante «Plus», che dispone di una gestione accessi aggiuntiva, permettendo di gestire le autorizzazioni a livello di documento o cartella.

1.2. GeBüV

Il regolamento sulla tenuta e conservazione dei libri contabili (GeBüV) di aprile 2002 (stato al 1° gennaio 2013) si basa sull'articolo 958f paragrafo 4 del Codice delle Obbligazioni svizzero. Il GeBüV elenca i libri da tenere e stabilisce principi generali per la loro gestione e conservazione. Inoltre, stabilisce principi per la corretta conservazione e fornisce indicazioni sugli strumenti di memorizzazione delle informazioni e le procedure ammesse. GeBüV è suddiviso in cinque sezioni:

1. Libri da tenere - libro mastro e, a seconda della natura e dimensione dell'attività, anche libri ausiliari
2. Principi generali di corretta gestione e conservazione dei libri, integrità, documentazione
3. Principi per la corretta conservazione - dovere di diligenza, disponibilità, organizzazione, archivio
4. Supporti di informazione - Supporti di informazione ammessi, verifica e migrazione dei dati
5. Disposizioni finali - entrata in vigore e abrogazione del diritto precedente

La documentazione su GeBüV è disponibile online al seguente link:
https://www.fedlex.admin.ch/eli/cc/2002/216/it

2. Raccomandazioni operative di eArchiv

Di seguito sono riportate raccomandazioni operative che devono essere osservate quando si utilizza «eArchiv». Questi requisiti possono essere soddisfatti nell'ambito dell'offerta principale di KLARA.

2.1. Formati di archiviazione

KLARA eArchiv può memorizzare e archiviare una varietà di formati. Per l'archiviazione a lungo termine e l'archiviazione conforme a GeBüV, è importante utilizzare formati di archiviazione a lungo termine. KLARA eArchiv garantisce l'archiviazione conforme a GeBüV esclusivamente con il formato «PDF/a», pertanto converte tutti i file PDF in PDF/a.

2.2. Autenticazione e autorizzazione

L'assegnazione e la gestione delle autorizzazioni di accesso generali possono essere effettuate esclusivamente all'interno di KLARA. Per l'assegnazione e la gestione delle autorizzazioni di accesso a livello di documento o cartella è necessaria l'opzione «eArchiv» nella variante «Plus».

La gestione dell'identità degli utenti può essere effettuata esclusivamente dal cliente al di fuori di KLARA. A questo proposito, il cliente è responsabile per l'organizzazione e la documentazione appropriata, o può fare riferimento alle direttive e documentazioni esistenti.

Inoltre, è importante assicurare che tutte le persone fisiche che utilizzano KLARA come utenti di un'azienda ricevano un profilo utente personale e siano registrate come utenti di un'azienda all'interno dell'offerta principale di KLARA. Altrimenti, non è garantito che l'accesso anonimo sia prevenuto.

Il cliente è responsabile per l'organizzazione, la documentazione e la gestione delle autorizzazioni di accesso, in particolare per la revoca dei diritti di accesso al momento della cessazione di un dipendente.

Tutte le password rilevanti degli amministratori (utenti) per l'accesso a KLARA e la gestione all'interno di KLARA devono essere gestite dal cliente attraverso una procedura documentata. L'uso dei profili utente o delle password, per quanto riguarda l'accesso a informazioni critiche, deve essere organizzato secondo il principio delle quattro occhi. Questo vale anche per il reset delle password.

La distribuzione dei profili utente amministrativi (utenti) deve essere regolarmente controllata dal cliente all'interno dell'offerta principale di KLARA e adeguata se necessario.

Ogni utente di KLARA che debba accedere a documenti archiviati conformemente a GeBüV (o al sistema stesso) deve essere registrato obbligatoriamente all'interno dell'offerta principale di KLARA. KLARA non ammette utenti anonimi.

2.3. Periodi di conservazione

I periodi di conservazione dei documenti d'archivio secondo GeBüV devono essere determinati dal cliente. Si noti che possono derivare periodi da altre disposizioni regolamentari o legali che vanno oltre i requisiti di GeBüV (ad esempio, responsabilità del prodotto). Il rispetto dei periodi è responsabilità del cliente e non è regolato/verificato da «eArchiv».

Leggi possibili che influenzano i periodi di conservazione:

- Legge sulla protezione dei dati
- Legge sul secondo pilastro dei fondi pensione
- ecc.

2.4. Verifica dell'integrità

Il cliente è obbligato a verificare che l'integrità sia mantenuta quando si carica un file da una fonte esterna prima che il file sia archiviato. KLARA effettua in eArchiv, ad ogni accesso dell'utente (max 1x al giorno), un controllo dell'integrità che procede come segue:

- Verifica della validità della firma dei documenti confrontando gli hash della richiesta con un hash appena generato del documento per 100 documenti
- Verifica che i documenti possano essere decifrati
- Verifica che ogni documento abbia una firma digitale
- Verifica della corrispondenza delle firme digitali
- In caso di errore durante questa verifica, viene attivato un allarme interno per identificare la causa del problema e risolverlo
- Successivamente, gli hash dei documenti interessati vengono ricalcolati per garantire la firma

2.5. Esportazione di documenti

KLARA fornisce, durante l'esportazione di documenti dall'archivio, i formati originali, le firme elettroniche e i log file.

I dati esportati sono disponibili per il cliente per 14 giorni tramite un link di download personale e possono essere decifrati solo tramite una password precedentemente definita da un profilo utente amministrativo (utente).

In caso di esportazione dei dati d'archivio, KLARA raccomanda un controllo dei documenti scaricati per completezza e correttezza.

3. Caratteristiche tecniche

3.1. Conservazione dei dati

Tutti i documenti nei formati originali (PDF/A), ulteriori documenti e informazioni sui documenti e i log file sono memorizzati da KLARA in Google Cloud Storage in Svizzera con ridondanza multipla. I documenti nei formati originali sono criptati specificamente per il cliente per proteggerli da accessi e modifiche non autorizzati.

La sicurezza dei dati è garantita con la procedura di backup usuale, già impiegata da KLARA Business AG.

3.2. Backups

Il backup dei dati avviene in più modi:

Snapshots
- Viene creato quotidianamente uno snapshot del disco dati del database. Questi snapshot hanno una durata di 14 giorni.

Database di standby
- I file WAL dal database principale vengono memorizzati nello storage WAL.
- Un database di standby secondario legge i file WAL dallo storage WAL e viene così mantenuto aggiornato.

Backup completi su server di backup
- I backup completi settimanali vengono creati dal database di standby e inviati al server di backup; i file WAL vengono sincronizzati dallo storage WAL al server di backup.

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

3.3. Ripristino

A seconda del problema affrontato da KLARA, si attuano i seguenti procedimenti di ripristino:

I dati (disco rigido) del database principale sono danneggiati.

- I dati del server del database di standby vengono duplicati e utilizzati per il database principale.

I dati (disco rigido) sia del database principale che del database di riserva sono danneggiati.

- Viene utilizzato l'ultimo snapshot del disco rigido del database principale come punto di partenza.
- Tutti i WAL generati da questo snapshot vengono applicati.
- Il disco dati risultante viene duplicato e utilizzato per il server di standby.

I dati (disco rigido) sia del database principale che del database di standby sono danneggiati, e tutti gli snapshot sono danneggiati.

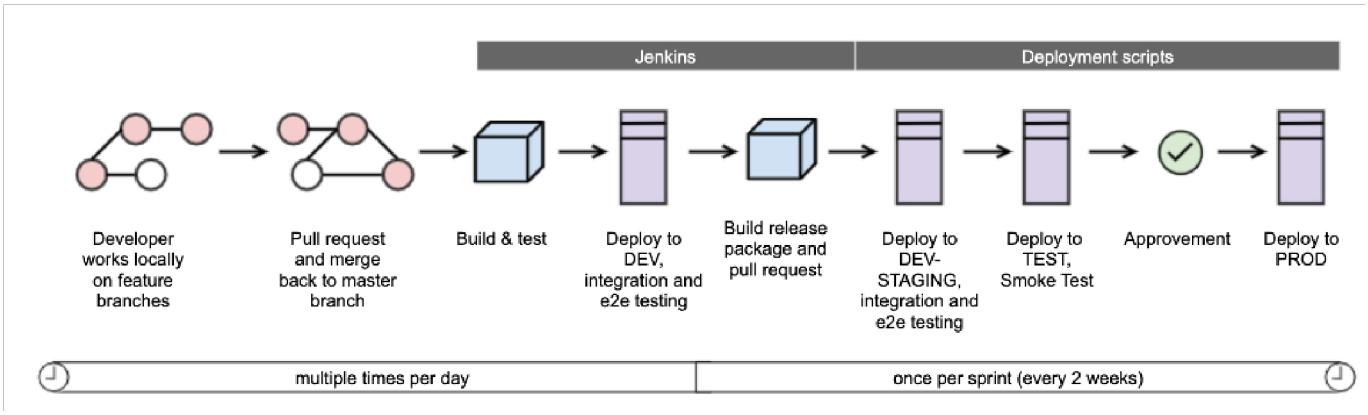
- The last full backup of the database is taken as the starting point.
- All WALs created since this backup are applied.
- The resulting data disk is duplicated and used for the standby server.

Tutti i dati vengono danneggiati nel progetto GCP.

- I server dei database principale e di standby vengono ricostruiti.
- Viene utilizzato come punto di partenza l'ultimo backup completo dei dati nel progetto GCP separato. Tutti i WAL creati da questo backup vengono trasferiti dal progetto GCP separato.

3.4. Processo di cambiamento

Prima che una nuova versione di un software venga messa in operazione da KLARA, essa passa attraverso diverse fasi di test per assicurare la compatibilità all'indietro e un funzionamento senza errori. L'immagine seguente illustra la procedura seguita da KLARA:



4. Varianti

4.1. Basic

«eArchiv» nella fornitura standard «Basic» include una serie di caratteristiche che consentono un funzionamento conforme alle normative legali di conservazione di un archivio documentale elettronico.

Le funzionalità incluse nel pacchetto standard di «eArchiv» comprendono le seguenti opzioni:

- Tutti i documenti vengono memorizzati in modo sicuro (criptati) e possono essere visualizzati solo dal cliente.
- Tutte le modifiche e gli accessi ai documenti (metadati) vengono registrati e memorizzati.
- Le modifiche sono collegate tra loro mediante un procedimento blockchain.
- Tutte le modifiche al documento sono visualizzabili dall'utente come cronologia nell'interfaccia utente.
- Ogni documento è marcato con una firma esterna e le informazioni relative sono mostrate all'utente nell'interfaccia utente.
- Controllo regolare dell'integrità come specificato nella verifica dell'integrità.

4.2. Plus

L'opzione aggiuntiva «Plus» include tutte le funzionalità presenti nella fornitura standard «Basic». Tuttavia, questa opzione offre anche la possibilità di definire diritti di accesso a livello di documento o cartella. Questo è stato implementato nel modo seguente:

1. Ogni oggetto di business (documento o cartella) può essere assegnato a una o più classi di sicurezza.
2. Ogni utente può essere assegnato a una o più classi di sicurezza.
3. Un utente ha accesso agli oggetti di business che corrispondono almeno a una delle classi di sicurezza a lui assegnate.
4. L'amministratore del profilo aziendale in KLARA Business ha sempre accesso a tutti i documenti.

5. Registrazioni

Le modifiche ai documenti e alle cartelle sono tracciate attraverso la creazione di eventi che documentano le modifiche ai metadati del documento o della cartella. I seguenti cambiamenti ai metadati vengono tracciati e menzionati specificamente nell'evento (i valori sono criptati):

- Cambiamenti del tipo di documento
- Cambiamenti al collegamento di cartelle di un documento
- Modifiche ai tag

An event consists of the following data:

- Id (ID unico)
- auditData (cambiamenti al tipo di documento, collegamento di cartelle o tag)
- eventDateTime (timestamp)
- eventDescription (azione dell'utente)
- eventFingerprint (hash calcolato)
- eventStatus (riuscito o fallito)
- eventSubType (oggetto; documento, file, metadati, ecc.)
- eventType (azione)
- objectId (documentId o folderId)
- objectType (documento o cartella)
- softwareModule (modulo in cui sono state fatte le modifiche)
- tenantId (cliente)
- transactionId (usato per raggruppare diversi eventi realizzati con un'azione dell'utente)
- Utente (email)

Sull'interfaccia utente, l'utente può vedere tutte le modifiche fatte al documento, quando sono state fatte e da chi sono state fatte.

5.1. Registrazioni generali

5.1.1. Accesso eArchiv

Ogni accesso a eArchiv viene registrato.

5.2. Registrazioni documenti

Tutte le modifiche alle informazioni dei documenti (metadati) e gli accessi ai documenti vengono registrati e memorizzati. Le registrazioni vengono eseguite all'interno di KLARA e alla fine del giorno vengono salvate su Google Cloud Storage come file .csv.

5.2.1. Accesso ai documenti

Ogni accesso a un documento viene registrato.

5.2.2. Ricezione del documento

Quando un cliente riceve un documento, il suo ricevimento viene registrato. Se il documento viene fornito già con un tipo di documento predefinito, questo viene menzionato nella registrazione.

5.2.3. Caricamento del documento

Quando un utente carica manualmente un documento nell'archivio, questo caricamento viene registrato. Se il documento viene caricato direttamente in una cartella d'archivio esistente, questa viene menzionata nella registrazione.

5.2.4. Elaborazione del documento

Dopo che un documento è stato consegnato al cliente, viene elaborato da KLARA e arricchito con ulteriori informazioni. Durante questa elaborazione, il documento viene, tra l'altro, firmato e il tipo di documento viene letto (a meno che non sia già definito da terzi). La firma e la definizione del tipo di documento vengono registrate.

5.2.5. Caricamento file successivo

All'interno di KLARA, un documento può consistere solo di informazioni sul documento e non avere un file di riferimento. Il file di riferimento, tuttavia, può essere aggiunto successivamente alle informazioni del documento. Questo caricamento file successivo viene registrato.

5.2.6. SmartLetter

Come forma speciale di lettera, KLARA offre ai suoi clienti un cosiddetto «SmartLetter», che può essere consegnato solo digitalmente e offre al destinatario la possibilità di inviare una risposta come reazione al contenuto. Il «SmartLetter» viene salvato all'interno di KLARA come PDF/A, firmato e marcato con un timestamp. Il ricevimento di questa forma speciale di lettera e il momento della risposta da parte del destinatario vengono registrati.

5.2.7. Archiviazione del documento

Quando un documento viene archiviato da un utente, questo viene registrato. La referenza alla cartella in cui il documento è stato salvato viene menzionata nella registrazione.

5.2.8. Modifiche al documento

Qualsiasi cambiamento alle informazioni del documento (metadati) viene registrato. Questi includono modifiche a:

- Titolo
- Descrizione
- Tipo di documento
- Importo (per le fatture)
- Data di scadenza (per le fatture)
- Tag

Se vengono apportate modifiche al tipo di documento o ai tag, queste vengono menzionate nella registrazione.

5.2.9. Spostamento del documento

Un documento può essere spostato all'interno dell'archivio da una cartella all'altra. Inoltre, è possibile che un documento venga copiato e posizionato in un'altra cartella. Lo spostamento e la copia di un documento vengono registrati. In entrambe le operazioni, la referenza alla cartella in cui il documento è stato copiato/spostato o dalla cartella da cui è stato spostato viene menzionata nella registrazione.

5.2.10. Cancellazione del documento

Quando un documento viene cancellato da un utente, viene spostato in un cestino. Il documento rimane visibile nel cestino per 30 giorni prima che venga eliminato definitivamente dal sistema. Alternativamente, l'utente può anche eliminare manualmente il documento in modo definitivo. Lo spostamento del documento nel cestino e l'eliminazione automatica o manuale definitiva del documento vengono registrati.

5.2.11. Ripristino del documento

Un documento spostato nel cestino può essere ripristinato da un utente. Il ripristino viene registrato di conseguenza. Se il documento viene ripristinato in una cartella, la referenza alla cartella in cui il documento è stato ripristinato viene menzionata nella registrazione.

5.2.12. Annullamento delle azioni

Alcune azioni sui documenti possono essere annullate dall'utente. Queste includono:

- Archiviazione
- Cancellazione
- Copia
- Spostamento

Quando un'azione viene annullata, questa viene registrata. Nell'annullamento dell'archiviazione e della copia di un documento, la referenza alla cartella in cui il documento doveva originariamente essere archiviato/copiato viene menzionata nella registrazione.

5.3. Registrazioni cartelle

Tutte le modifiche alle informazioni delle cartelle (metadati) e gli accessi alle cartelle vengono registrati e memorizzati. Le registrazioni vengono eseguite all'interno di KLARA e alla fine del giorno vengono salvate su Google Cloud Storage come file .csv.

5.3.1. Creazione di cartelle

Quando un utente crea una cartella nell'archivio, la creazione viene registrata. Nel caso della creazione di una sottocartella, viene inoltre menzionata la referenza alla cartella superiore nelle registrazioni.

5.3.2. Accesso alle cartelle

Ogni accesso a una cartella da parte di un utente viene registrato.

5.3.3. Spostamento delle cartelle

Una cartella può essere spostata all'interno dell'archivio da una cartella radice a un'altra cartella o da una cartella a un'altra. La referenza alla cartella superiore nelle registrazioni viene menzionata nel caso in cui la cartella venga spostata o dalla cartella da cui è stata spostata.

5.3.4. Modifica del nome

La modifica del nome di una cartella viene registrata.

5.3.5. Cancellazione della cartella

Quando un utente cancella una cartella, questa insieme a tutti i documenti in essa contenuti viene spostata in un cestino. La cartella e il suo contenuto rimangono visibili nel cestino per 30 giorni prima che vengano eliminati definitivamente dal sistema. In alternativa, l'utente può anche eliminare manualmente la cartella e/o il suo contenuto in modo definitivo. Lo spostamento della cartella nel cestino e l'eliminazione automatica o manuale definitiva della cartella vengono registrati.

Eccezione: se un documento è salvato in più cartelle e poi una di queste cartelle viene cancellata, il documento non viene spostato nel cestino.

5.3.6. Ripristino della cartella

Una cartella spostata nel cestino può essere ripristinata da un utente. Il ripristino viene registrato di conseguenza. Se la cartella viene ripristinata in un'altra cartella, la referenza alla cartella in cui la cartella è stata ripristinata viene menzionata nella registrazione.

6. Integrità dei documenti e delle registrazioni

6.1. Uso di firme digitali

KLARA utilizza firme digitali e timestamp per aumentare la validità giuridica dei documenti archiviati e dei loro log. I documenti e le registrazioni sono firmati digitalmente al momento della loro creazione. Così, tutti i documenti e le registrazioni all'interno di «eArchiv» ricevono un timestamp.

Le firme digitali sono generate da fornitori ufficiali esterni e vengono associate come file di firma separati al documento stesso, memorizzati nello stesso luogo di archiviazione. Come fornitori ufficiali esterni vengono utilizzati «Swiss TSA», gestito da BIT, e «FreeTSA.org». Di norma, viene utilizzato «Swiss TSA» e «FreeTSA.org» come backup in caso di indisponibilità di «Swiss TSA».

Alla fine della giornata, tutte le registrazioni per cliente vengono esportate in un file .csv. Viene generato un hash del file e il file stesso viene memorizzato per cliente su Google Cloud Storage. Gli hash di tutti i file esportati vengono raccolti in un altro file. Questo nuovo file generato è marcato con un timestamp e conservato specificatamente su Google Cloud Storage.

6.1.1. Integrity Check

KLARA verifica la validità della firma ad ogni accesso dell'utente (massimo 1x al giorno) e confronta anche l'hash della richiesta con un hash appena generato del documento. Un documento è considerato integro solo se la firma è valida e i due hash corrispondono.

Se gli hash non corrispondono o la firma non è più valida, viene creato un allarme interno e la KLARA Business AG verifica quale sia la causa della non corrispondenza e la corregge.

Con questo controllo dell'integrità vengono effettuati i seguenti test:

1. Verifica che i documenti possano essere decifrati.
2. Verifica che ogni documento abbia una firma digitale
3. Verifica della corrispondenza delle firme digitali.

6.2. Uso della tecnologia blockchain

Per garantire l'integrità di ogni singola registrazione, viene calcolato un hash di tutti i dati delle registrazioni attuali e dell'hash delle registrazioni precedenti. In questo modo, le singole registrazioni sono collegate tra loro in una «catena». Questo processo viene eseguito durante il giorno non appena viene generata una registrazione.

Tutti gli hash vengono ricalcolati giornalmente e confrontati con gli hash originali. Le registrazioni sono considerate integre solo se gli hash ricalcolati corrispondono agli hash originali. I processi successivi vengono avviati solo quando l'integrità delle registrazioni può essere garantita.

Se gli hash non corrispondono, tutti i processi relativi alle registrazioni di «eArchiv» vengono interrotti e viene creato un allarme interno (esclusa la creazione delle registrazioni). La KLARA Business AG quindi verifica quale sia la causa della non corrispondenza e la corregge. Solo dopo la correzione, i processi successivi vengono riavviati.

In caso di interruzione, KLARA tiene un registro degli errori e lo memorizza all'interno di «eArchiv».

7. Osservazioni generali

Il funzionamento di «eArchiv» avviene sulla piattaforma Google Cloud (GCP) e tutti i dati vengono memorizzati su Google Cloud Storage.

Le certificazioni della piattaforma Google Cloud possono essere consultate qui.

KLARA Business AG è un'azienda certificata ISO27001.