

Technical System Description for Processing Digital Receipts

Table of Contents

CHANGE HISTORY	4
TABLE OF FIGURES	5
GLOSSARY.....	5
1. INTRODUCTION	7
1.1. RESPONSIBILITIES	8
1.2. REQUIREMENTS.....	8
2. TYPES OF DOCUMENTS	8
3. GENERAL PROCESS DESCRIPTION	8
3.1. RECORDING OF EXPENSES, INVOICES AND CARD TRANSACTIONS	9
3.2. APPROVAL	11
3.3. FINANCE REVIEW	12
3.4. FINANCE POSTING	13
3.5. SYSTEM CONTROLS	14
4. ACCESS TO THE SYSTEM	14
4.1. ROLE AND AUTHORISATION CONCEPT	15
4.1.1. <i>Submitter</i>	15
4.1.2. <i>Assistant</i>	15
4.1.3. <i>Manager</i>	16
4.1.4. <i>Finance Review Team</i>	16
4.1.5. <i>Audit Team</i>	16
4.1.6. <i>Customer Administrator</i>	16
4.1.7. <i>Yokoy Administrator (Technical Administrator with Full Access)</i>	16
4.1.8. <i>Yokoy Support</i>	17
4.2. ACCESS CONTROL POLICY	17
5. DATA SECURITY MEASURES.....	17
5.1. PHYSICAL ACCESS CONTROL (IN THE DATA CENTRE)	17
5.2. LOGICAL ACCESS CONTROL	17
5.3. TRANSMISSION CONTROL.....	18
5.4. INPUT CONTROL	18
5.5. AVAILABILITY CONTROL.....	18
5.6. SEPARATION REQUIREMENTS	18
6. CREATION AND PROCESSING OF DATA.....	19
6.1. DOCUMENT CONTENTS	19
6.2. ENTERING THE RECEIPT	20
7. INDEXING OF THE DATA	20
8. TRACKING DATA	20
8.1. SEARCH FUNCTION	21
8.2. PROCESS FLOW	21

8.3.	DATA EXPORTS	21
9.	IMMUTABILITY OF THE DATA	22
9.1.	NEED FOR CONTROL AND CORRECTION	22
9.2.	SPECIAL NEED FOR CORRECTION	22
10.	LEGAL NOTES	22
10.1.	AUSTRIA	23
10.2.	GERMANY	23
10.3.	NETHERLANDS	25
10.3.1.	<i>Retention Period for the Records</i>	<i>26</i>
10.3.2.	<i>Digital retention</i>	<i>26</i>
10.4.	SPAIN	26
10.5.	SWITZERLAND	27

Change History

Name	Date	Change
v0.1	31.01.2023	Initial draft
v0.2	06.02.2023	Internal review
v1.0	21.02.2023	Final approval - First version

Table of Figures

FIGURE 1: FUNCTIONAL CONCEPT OF YOKOY	7
FIGURE 2: AI LOGICS FOR DATA EXTRACTION	10
FIGURE 3: CAPTURING EXPENSES.....	11
FIGURE 4: APPROVING EXPENSES.....	12
FIGURE 5: REVIEWING EXPENSES	13
FIGURE 6: EXPORT LOG.....	14
FIGURE 7: PROCESS FLOW OF EXPENSE RECEIPTS	20
FIGURE 8: AUDIT TRAIL.....	21
FIGURE 9: REGULATORY CRITERIA (SOURCE: BMF DE)	25

Glossary

Explanation of important terms and abbreviations.

Term	Definition
AI	Artificial Intelligence.
BDSG	German: <i>Bundesdatenschutzgesetz</i> . Federal Data Protection Act, that together with the data protection acts of the German federated states and other area-specific regulations, governs the exposure of personal data, which are manually processed or stored in IT systems.
BMF	German: <i>Bundesministerium der Finanzen</i> . Federal Ministry of Finance. Legislative authority in Austria and Germany.
EStG	German: <i>Einkommensteuergesetz</i> . Income Tax Act. Regulates the taxation of the income of natural persons in Germany.
GCP	Google Cloud Platform. A suite of cloud computing services offered and operated by Google.
GoBD	German: <i>Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff</i> . Principles for the proper management and storage of books, records, and documents in electronic form and for data access. Administrative regulation in Germany.
ISO	International Organization for Standardization.
OCR	Optical Character Recognition. Electronic or mechanical conversion of images of typed, handwritten, or printed text into machine-encoded text.
RBAC	Role-Based Access Control. Approach to restricting system access to authorized users.

Term	Definition
REST	Representational State Transfer. Software architectural style that describes the architecture of the Web.
SaaS	Software as a Service. A software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted.
TLS	Transport Layer Security. A cryptographic protocol designed to provide communications security over a computer network.
VAT	Value-Added Tax.

1. Introduction

Yokoy Switzerland Ltd and all Yokoy entities in the different countries (“Yokoy” or “the Company”), is a Swiss technology service provider focused on automating corporate spend management. With its AI-based platform, Yokoy addresses corporate spend in its entirety - from handling expenses and vendor invoices to managing



smart company cards.

Figure 1: Functional concept of Yokoy

Yokoy all-in-one spend management platform is targeted to medium businesses and large corporations, and consists of three main service offerings:

- **Expense management.**
Uploading, editing, and submitting expense reports with automated expense report creation based on pictures or document uploads (manual entries for per diems and mileage claims).
- **Invoice processing.**
Uploading of supplier invoices and auto-creation of forms in order to process supplier invoices via workflow.
- **Corporate cards.**
Physical and virtual card solutions to match transactions directly with receipts, enabling full transparency and spend control with a maximum of flexibility.

The platform is cloud-based and serviced from data centers operated by Google Cloud Platform (GCP) in the EU according to GDPR with a strict physical security and control policy in place, particularly:

- St. Ghislaine, Belgium
- Frankfurt, Germany
- Zurich, Switzerland

As a SaaS offering, a single version of the software is used by all customers. However, individual customer requirements can be met via configuration settings so that the platform can adapt to different needs.

This document describes how the recordable and retainable data is generated, processed, and stored in Yokoy. It can also be added to legal documents which are required in some countries.

1.1. Responsibilities

Yokoy is responsible for the technical processing of the digital receipts. Based on the incoming receipts, Yokoy will read the contained data and try to match expense categories configured in the system.

It is customers responsibility to offer suitable categories and to check plausibility and correctness before the Finance postings are released. Yokoy cannot interpret whether facts on the receipt are plausible or legally compliant. Yokoy will not be liable for incompliant or fraudulent transactions being posted to Finance.

This document describes the handling of receipt storage inside Yokoy.

1.2. Requirements

The implementation, operation and support of an Expense solution requires the organizational readiness of the client. Key responsibilities should be defined and in place. For operation, a skilled Finance team should be in place for audit and support. Travel policies or accepted policies per country should be in place. Payment methods for travel services should be known in all countries involved. Suitable technical administrators for monitoring of the data flows should be available.

When submitting expenses, all users are expected to have a valid email address, access to the Yokoy mobile (or web) app, and a camera or scanner to digitize printed receipts.

2. Types of Documents

The objects of digitization are all documents originally available or received in paper form or electronic form that have a document function in the sense of commercial and/or tax accounting or recording obligations and are therefore subject to a retention obligation.

The object of digital archiving is all documents that are originally received in paper or electronic form and are archived in the designated system.

Typical formats used in the process are:

- Paper receipts issued by merchant (e.g., hotel bill, taxi receipt, among others).
- Electronic receipts (e.g., car rental bills, travel agency invoices, rail tickets, among others) in various formats (e.g., mail body, structured PDF/A, regular PDF) sent by merchant or handling agent.
- Electronic invoices sent by merchant or handling agent (e.g., monthly collective invoices for car rental or travel agency).

3. General Process Description

The following representation of the process is ideal-typical and can vary in the design of the sequence and number of process steps (e.g., in the number of release stages) depending on the customer setting.

Yokoy has two user frontends in place, which are offering same functions:

- **Yokoy Mobile App.**

A mobile application that scans receipts using a photographic process and provides receipt image data for downstream systems. The receipt image data is stored as a PDF document or as an image (JPEG/PNG). The mobile application also allows uploading existing PDF files and recording expenses for which no receipt is required (e.g., per diems and mileage allowance).

- **Yokoy Web App.**

A browser-based application where receipts can be added and managed.

3.1. Recording of Expenses, Invoices and Card Transactions

The descriptions and screenshots in this section refer to the mobile app. However, uploads and subsequent actions can also be performed in the web app for expenses and invoices, whereas transactions get imported from Card Scheme providers or other external parties (e.g., banks). The use of the different input options is a client decision.

Available input channels for electronic receipts are:

- Send to Yokoy by mail (sender's mail address must be registered mail address in Yokoy).
- Upload a locally stored document (picture, PDF, multi-page) using the app (mobile or web).
- Connect an email inbox to Yokoy (used for invoice module).

Available input channels for paper receipts are:

- Taking a picture with the mobile app, using the device camera with immediate upload to the app (built in function).
- Scanning a Paper Receipt with an external device, then adding it to local storage and uploading it via web app.
- Scanning a multi-page invoice with an external device, then adding it to local storage and uploading it via web app.
- Scanning a Paper Receipt with an external device, then sending it directly to Yokoy by e-mail.
- Scanning a multi-page invoice with an external device, then sending it directly to Yokoy by e-mail.
- E-invoicing solutions that are connected to Yokoy.

Available input channels for transactions are:

- For Yokoy cards, transactions are imported via data provided by Marqeta (processor).
- For external company cards, input is in general provided by partners such as banks, card schemes etc.

After uploading to Yokoy, the system processes the document and extracts the data (i.e., transaction date, transaction type, category, and VAT, among others) through the AI-based OCR. Sample below for an expense.

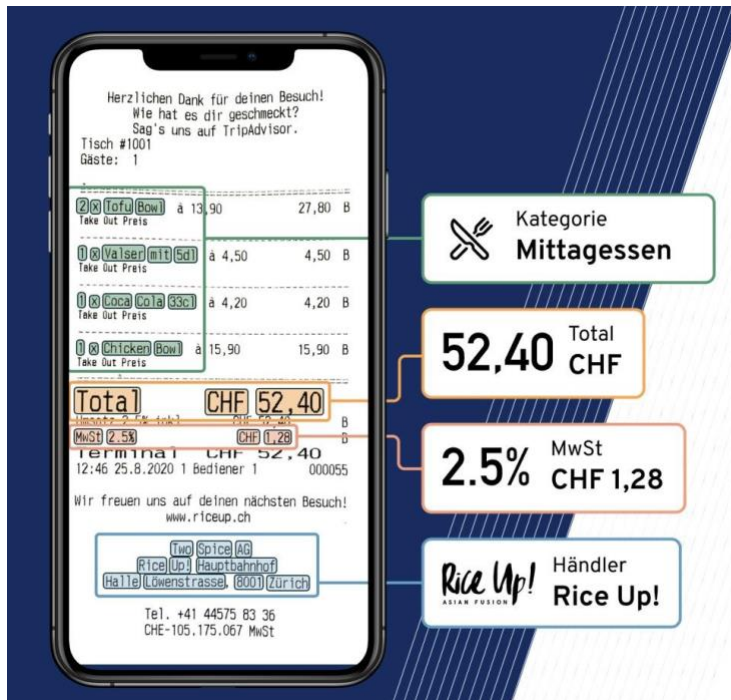


Figure 2: AI logics for data extraction

After Yokoy extracts the data, the user validates it and is allowed to correct or make any changes needed. Required content can be set to mandatory as part of the customer configuration.

For the expense module, per diems and mileage allowances can be added without a receipt in the standard version. For other transactions, customer can choose whether to allow transactions without receipt or not.

In case of card transactions from a company-billed card, the user gets regular email notifications to upload the respective receipt and start the process. The frequency of these notifications can be configured by to monthly, weekly, or daily.

When an expense is submitted that was paid by company card, Yokoy will try to match it automatically with the corresponding card transaction. An automatic match is performed if card, expense date and transaction date are identical, and the currency and amount of the transaction is identical with that of the expense (or deviates within a configurable range). In addition to automatic matching, a Submitter or Finance user can also manually match a submitted transaction with the corresponding expense if the amounts are within the configurable range of deviation. In case a transaction cannot be matched with an expense because the amounts exceed the allowed range of deviation, it is possible for a technical user to force match the transaction with the expense.

Once the user has completed entering information, an overview of the output is displayed, and the user can save or submit the output. The output appears in the dashboard overview. Once the output is saved, standard and customized warnings can be displayed and are visible to all stakeholders (user, auditor, manager, accounting). This is custom configuration.

If there is no custom workflow configuration, the output is sent directly to the Finance Review team. As long as the output has the status "Pending", the user can still edit the information. As soon as the Finance Review team releases the transaction for payment, the user has read-only access.

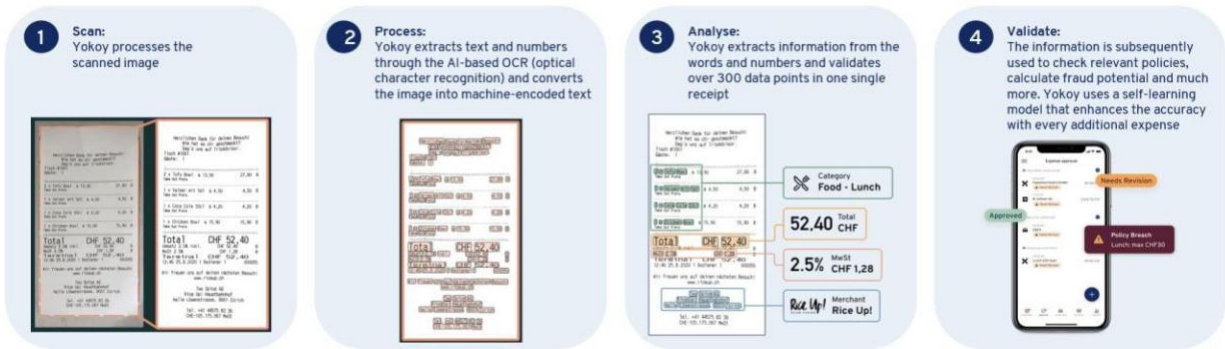


Figure 3: Capturing expenses

3.2. Approval

After submission, expenses, invoices and / or transactions get forwarded to a responsible manager for approval. Additionally, certain transaction can be excluded from approval based on warning level or payment type. This can be configured by the customer.

Managers (approvers) only have access to their team's expenses. Approvers have the option of mass-approving or -rejecting employee expenses.

The controls that are carried out by the Managers typically consist of verifying:

- If the expense / invoice / card transaction is compliant with the company policies.
- The expenditure is justified and correctly accounted for (e.g., cost object split, category, etc.).

At this point, the Manager can approve transactions or reject with comment.

Certain transactions can be flagged with individual warnings to ensure company policy. Custom approval flows are available on demand, to be implemented by the Yokoy engineering team.

Approved items get forwarded to Finance review, rejected items get back to the Submitter for correction. The applicant must make the corrections and then re-submit the statement.

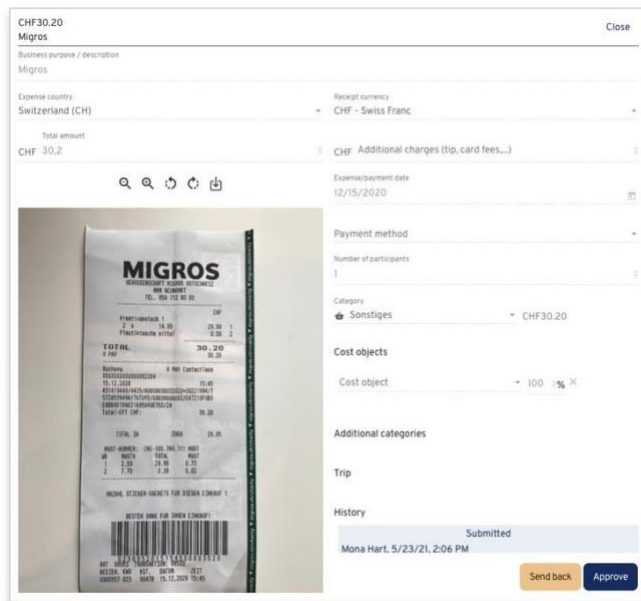


Figure 4: Approving expenses

3.3. Finance Review

Depending on customer's configuration, all items or only some of them are forwarded to Finance for review before getting released for payment.

The financial review takes place after management approval or directly after submission if approval is skipped.

The Finance team can approve or reject transactions, optionally indicating a comment. The Finance team can also change all entries except for the amounts entered. The following tasks are performed:

- Check and edit data entries.
 - Check all data entries for correctness and, if necessary, make adjustments (only for expenses with warnings).
 - Finance users can change all information except for the total amount, receipt currency and additional charges.
- Check VAT.
 - Select the correct VAT rate/s and, if applicable, enter a VAT number in the expense report or the invoices item (only Finance users can do this).
- Send back to Submitter or approve.
 - In case one of the fields a Finance user is unable to edit contains errors, the transaction is sent back to the Submitter for revision, stating the reason in the comment field. The Submitter must make the corrections and then resubmit the statement.
 - If an invoice item / expense report violates a company policy, supplier rules or other policies, the expense/invoice can be rejected permanently, stating the reason in the comment field.
 - If the item is correct, Finance records its review and approval.

After Finance reviews, the data is made available for transfer to the appropriate financial systems. The actual payments do not take place in Yokoy.

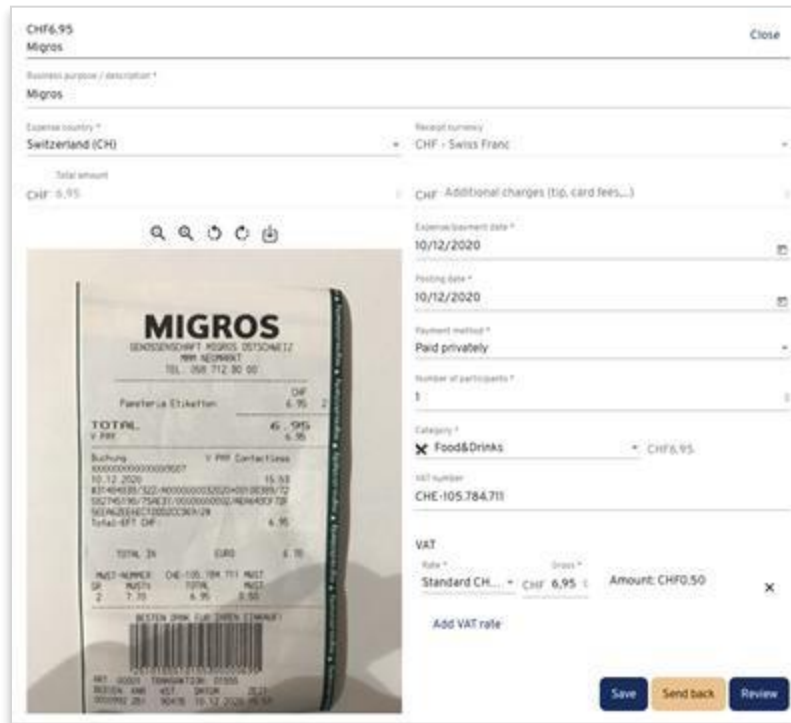


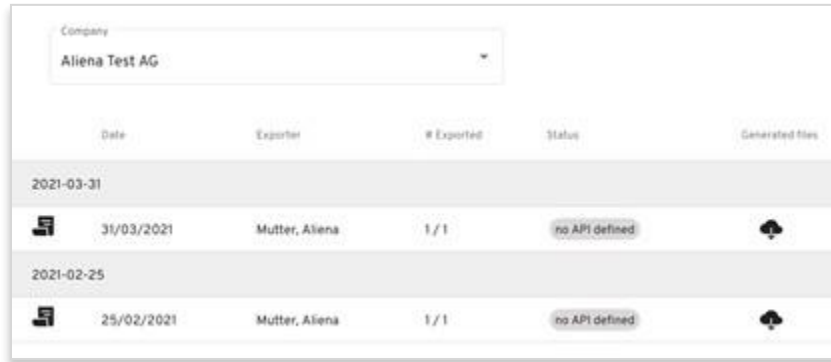
Figure 5: Reviewing expenses

3.4. Finance Posting

Once the expense is approved and reviewed, it can be exported to the Finance system. Yokoy supports various export formats with predefined interfaces to many ERP and Finance systems. Contained data may vary per target system.

Transaction data and receipt images can be handed over to Finance systems, where the Finance posting and reimbursement take place. The target system is entirely the responsibility of the client.

The full history of exports is visible in the export logs. Here, the transferred data can be manually extracted anytime for audit checks or other purposes.





Date	Exporter	# Exported	Status	Generated files
2021-03-31				
31/03/2021	Mutter, Aliena	1 / 1	no API defined	
2021-02-25				
25/02/2021	Mutter, Aliena	1 / 1	no API defined	

Figure 6: Export log

3.5. System Controls

Yokoy alerts all users (staff, audit team, managers, accounting) of any identified anomalies. These can be enabled/disabled at the client's request. The system controls appear as warnings and can block the approval of the output.

The standard system controls are the following:

- Duplicates. If Yokoy recognizes a receipt as an expense already submitted (based on currency, amount, datetime, and merchant), the expense report will be flagged. A Finance user can find the duplicate expense by searching for the expense ID listed in the warning.
- Issues with missing information.
- Country/currency reconciliation.
- Participant (e.g., an employee who was invited by another user to a business lunch registers a lunch expense himself on the same day).
- Invalid tax information (i.e., the tax information does not match the total amounts).
- Invalid tax rate (i.e., the determined tax rate does not match the tax rates of the country).

In addition to the system controls described, customized warnings can be configured and displayed in the outputs.

4. Access to the System

Users have access to the system exclusively via the application: access to the document data (and images) happens exclusively via the user interfaces offered in the system (browser-based or mobile app).

The user logs in with an e-mail address and a password. The described role concept ensures that the user can only access data and processes for which his role is authorized.

Integration into the customer's role authorization concepts is possible through customizable synchronization with Yokoy's user data model. Single Sign-On (SSO) is also possible, by integrating the customer Identity Provider (IdP). For example, Azure AD.

Login to the system is only possible for users who have already been created. Users can only be created by authorized persons who have the corresponding administrator rights on the platform. When logging in for the first time, the user is asked to create his or her password.

Yokoy stores logs of all user logins. These logs are application logs and therefore not accessible to the user via the user interface. However, these can be reviewed by Yokoy's Level 3 support team in case of a justified customer request.

Functions offered through the application provide for the possibility of making changes to the content in submissions only during the pre-established stages. The possibility to make changes only applies to the document data set, not to the image file.

System-level manipulation of document images is ensured through the strict application of security policies (including the regulation of access to data centers) and compliance with internationally recognized standards such as ISO 27001 according to which Yokoy is certified.

Local application installations are not present and therefore do not pose a risk of damaging documents and image data.

4.1. Role and Authorization Concept

Several roles are available for processing the data, with different access-levels for different tasks within the review, approval, and settlement processes.

By default, users have staff rights. In addition, users can be assigned several other profiles. Profiles can be set to all users or only a specific subset of them.

Customers can customize user profiles, with the possibility to control access to functions, visibility/modifiability of data (i.e., read, write, or read & write), type of data (invoices, expense reports and/or expenses), user groups (administrative units/departments), etc. The following sections describe the standard user profiles.

4.1.1. Submitter

By default, all users have Submitter permissions.

The Submitter users can:

- Submit transactions.
- Change their own transactions in the "Pending" state until they have passed the first approval step.
- Delete their own transactions in "Pending" state.
- Correct information and re-submit expenditure after it has been found to be "non-Compliant" in an audit stage.
- Monitor progress in the processing of their issues.

4.1.2. Assistant

Assistant's role needs to be assigned in the submitter's master data record. Assistants can perform a limited set of operations on behalf of other users. Assistants can assign one delegate assistant in case of absence or as permanent delegate.

The Assistant users can:

- Execute Submitter transactions on behalf of an assigned employee.

4.1.3. Manager

Manager's role needs to be assigned in the submitter's master data record. Managers act on submissions of their assigned employees. Managers can assign one delegate manager in case of absence or as permanent delegate.

The Manager users can:

- Approve transactions of assigned employees.
- Reject transactions of assigned employees.
- Add comments to approved or rejected transactions.
- See reports of transactions for assigned employees.

4.1.4. Finance Review Team

Finance Review roles must be actively assigned to the users.

Finance Review team can perform the following actions:

- Release for payment.
- Change transactions data (no change on amounts).
- Reject transactions.
- Reject transactions permanently.
- Access, query, and monitor transactions in each approval status.

4.1.5. Audit Team

The audit role needs to be assigned manually.

The Audit users can:

- Read all company's expenditure.
- Create and download reports.

4.1.6. Customer Administrator

The technical Administrator profile needs to be assigned manually.

It gives access to all master data, company master settings and integration settings.

4.1.7. Yokoy Administrator (Technical Administrator with Full Access)

The technical administrator profile does not give access to user outputs. Technical administrators with full access to a defined Company and its user group.

4.1.8. Yokoy Support

The Yokoy support team has access to the relevant customer data in the event of a malfunction. In addition, customers can choose to receive first and second level support from Yokoy. The support teams are based in the DACH area (Switzerland, Germany, and Austria).

4.2. Access Control Policy

Yokoy has an established Access Control Policy reviewed by external parties within the scope of ISO 27001. The policy applies to all systems, people and processes that constitute Yokoy's information systems, including board members, directors, employees, suppliers and any third party with access to Yokoy systems.

5. Data Security Measures

The following data security measures and the corresponding certifications mentioned above ensure that the data is protected against loss and unauthorized access and thus against falsification. The following paragraphs describe Yokoy's standard data protection.

Yokoy's data security architecture is certified with the data protection standards of ISO 27001 and documented on its Data Security Deck.

Yokoy classifies data according to its Information Classification Procedure and applies security and privacy controls associated with the data classification.

All access is based on least privilege and scoped to job function within the company and the service.

5.1. Physical Access Control (in the Data Centre)

Physical security and access control in the data center is responsibility of GCP. No Yokoy employee has physical access to the data center.

GCP data centers have extensive infrastructure and facility security certifications, including ISO 22301 (for business continuity management systems). More details on their safeguards and security features can be found at: <https://www.google.com/about/datacenters/data-security/>

5.2. Logical Access Control

Regarding Yokoy support users, Yokoy's Access Control Policy and User Access Management Process require access to Yokoy assets to be granted based on business justification, with the asset owner or line manager's authorization and limits based on "need-to-know" and "least privilege" principles.

In addition, the policies also address requirements for access management lifecycle including access provisioning, deprovisioning, authentication, authorization, and periodic access reviews.

Regarding customer's users, the customer is responsible for their adequate management by a delegated Administrator.

5.3. Transmission Control

All endpoints require authentication, data is encrypted before transmission and decrypted and verified on arrival. More information in the Yokoy Data Security Deck.

5.4. Input Control

Registration of users and time of the respective change in the Yokoy system.

The following criteria is applied when ingesting and recording financial-sensitive documents (such as receipts and invoices) at Yokoy in order to provide a reasonable level of assurance around integrity and authenticity of transactions:

- Identical reproduction (including colors).
- Conservation of documents in either PDF format or as images (JPEG/PNG).
- A timestamp of the documents, using an internal time source.
- A user identifier, matching the document submitter.
- Storage of up to 10 years, respectively the legal requirement in the country of the contracting party to enable an audit trail.

There is no application flow that allows for changes to digitalized receipts/invoices (either PDF or image) once submitted. Nonetheless, the supporting GCP storage service maintains simultaneously a “created” and “updated” timestamps that are checked for an exact match in order to guarantee the integrity of the documents.

5.5. Availability Control

Yokoy has an established Business Continuity Plan (BCP), compliant with ISO 27001, which outlines the existing safeguards and actions to take in the event of extended service outages caused by factors beyond control (e.g., natural disasters, man-made events), with the goal of restoring services to the widest extent possible in a minimum time frame. The plan is reviewed semi-annually and exercised on an annual basis.

Yokoy works with GCP as the cloud provider to store data. The database runs in high availability mode (multi-availability zone setting) to enhance durability and availability. In case of a disaster, Yokoy relies on the automated backups and database snapshots performed by GCP and tested regularly.

The digital archiving process at Yokoy ensures integrity and authenticity of the stored documents, for up to 10 years, respectively the legal requirement in the country of the contracting party to enable an audit trail.

5.6. Separation Requirements

Data separation measures have been fully implemented considering the multi-tenant nature of Yokoy offerings. This includes, among other aspects, the logical separation of clients within the application.

Additionally, access to application data is controlled using Role Based Access Controls (RBAC), so that only authorized users may logically access the intended data.

6. Creation and Processing of Data

Yokoy captures receipts issued for purchases made by employees from various suppliers. Yokoy provides support for PDF documents as well as images (JPEG/PNG). Depending on how the original receipt was created and submitted by the vendor to the employee, a document can enter the Yokoy platform in different ways:

- Paper receipts photographed with the Yokoy Mobile Apps (iOS and Android).
- Paper invoices/receipts scanned as PDF documents or as images (JPEG/PNG) with an external scanner, or native PDF invoices can be added as follows:
 - Uploaded via the Yokoy web and mobile apps.
 - Imported by forwarding an existing e-mail to the special Yokoy receipt e-mail address.

As soon as the digitized invoice/receipt is uploaded to Yokoy, an unalterable “created” timestamp is recorded in the underlying storage system and supports the document integrity controls.

- Receipts received/collected from the client's information system can be sent to Yokoy via a special API.
- Invoices sent directly to Yokoy by third party providers on behalf of the customer via Yokoy connectors (e.g., travel systems).

Employees enter their receipts in one of the above ways. This step is ultimately the responsibility of the user, and the time at which the receipts arrive in Yokoy can therefore vary from a few seconds to days or weeks later.

The document is sent to the Yokoy OCR module for automatic analysis and the app receives the suggested metadata for the output. The user can check and edit all fields before saving the output. The output metadata and the file are transferred to the Yokoy platform for storage.

Expenditure can then be reviewed, controlled, and approved via the Yokoy applications by client managers and accountants according to their internal processes on the subject.

Approved expenses can eventually be exported by the accounting and HR teams for downstream processing such as bookkeeping or employee reimbursement.

All data exchange between the Yokoy applications and the platform takes place via an encrypted connection (TLS 1.2 or higher) and requires full authentication and authorization of the user.

6.1. Document Contents

The captured document data includes the following elements:

- Seller.
- Date.
- Country of service provision.
- VAT rate.
- Amount (gross amount, net amount, VAT amount).
- Currency.
- Category.
- Payment method.

The image assigned to the document data is the entry point for an output. It cannot be deleted or exchanged. Only the entire output (document data content and image) can be deleted by the user as long as it is still in the "Pending" status.

6.2. Entering the Receipt

The following figure shows an overview of the flow of expense receipts and metadata within the Yokoy platform.

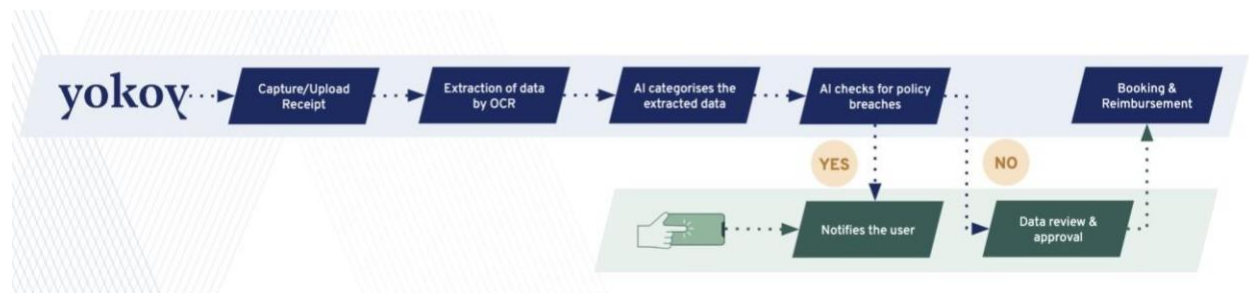


Figure 7: Process flow of expense receipts

The following technical components are essential to supporting the depicted flow:

- Yokoy platform: the central storage and processing location for all documents and data, fully hosted on GCP. All business transactions and customized configurations take place here.
- Yokoy REST API: a data interface that allows Yokoy applications (web and mobile) to communicate with the Yokoy backend. The same API also allows customers to automate operations on the Yokoy platform from their internal information systems.

7. Indexing of the Data

Each document is given a unique file ID. The metadata is closely linked to the document by storing the file ID together with its own generated unique ID (issue ID). This link can never be changed or deleted. In case of a user error related to the uploaded document (e.g., wrong document or blurred image), the output can be deleted and a new one must be created from the correct document.

The metadata of the outputs can be changed during some steps of the workflow by people with the appropriate rights. This may vary depending on the configuration of each client and is their responsibility.

Indexing is done at the level of the output metadata. The following indexing is used:

- Issue ID (unique identification criterion).
- User ID (unique ID of the owner of the output).
- ID of the user organization (ID of the company for which the user made the expenditure).

8. Tracking Data

The data can be found using various filters for a targeted search or various reporting options for the data.

Each issue has a unique identifier and can thus also be identified.

8.1. Search Function

In Yokoy, issues can be searched for according to various criteria.

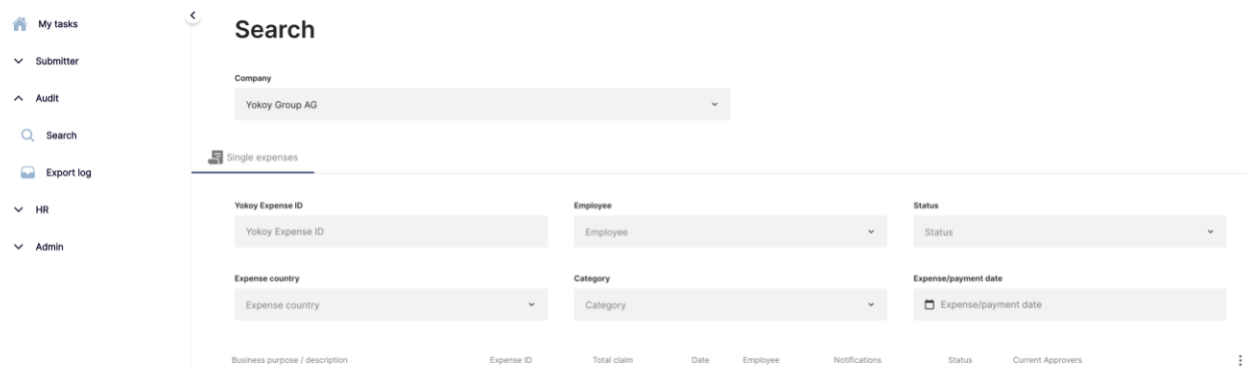
The most important of these are:

- First and last name of the user who owns the output.
- Date of creation.
- Issue date.
- Country or currency.
- Category.
- Type (i.e., standard costs, mileage allowance, daily allowance, flat rates).
- Payment method used.
- Approval status.
- Presence/absence of warnings.

8.2. Process Flow

Yokoy automatically records the history of changes per process in an audit trail. This log can be viewed via a special screen in the web app by all persons involved in the process who are allowed to access the outputs.

The audit trail also considers approvals performed in delegation mode and shows the user who granted the delegation and the holder who performed the step for him/her.



The screenshot shows the 'Search' interface in the Yokoy web app. On the left is a navigation menu with options: My tasks, Submitter, Audit, Search, Export log, HR, and Admin. The main search area includes a 'Company' dropdown menu set to 'Yokoy Group AG'. Below this is a 'Single expenses' section with several filter fields: 'Yokoy Expense ID' (text input), 'Employee' (dropdown), 'Status' (dropdown), 'Expense country' (dropdown), 'Category' (dropdown), and 'Expense/payment date' (calendar icon). At the bottom, a table header is visible with columns: Business purpose / description, Expense ID, Total claim, Date, Employee, Notifications, Status, and Current Approvers.

Figure 8: Audit trail

8.3. Data Exports

Various export formats are available as an alternative to displaying individual issues.

Exports can group any number of outputs that the user has access to and can include the metadata, the receipts or both.

Yokoy can also provide specific exports to create an analysis for specific expense types and use cases. For example, the mileage allowance export calculates a summary of all mileage allowance expenses for an employee over a year and calculates reimbursement data for the same period.

9. Immutability of the Data

As far as the immutability of data is concerned, the basic rule is that image data cannot be changed at any time. Similarly, the link between a document and its metadata cannot be changed or deleted.

Depending on the process step, expenditure metadata can be changed, either by the owner, by designated managers, or a Finance team member. This applies particularly to the need for changes/corrections during the audit step. From the time of approval by the manager until the final settlement/reimbursement step, the metadata can no longer be changed.

9.1. Need for Control and Correction

The output process includes the requirement to make changes to the output metadata at defined process points.

On the one hand, the user has the duty of care to scan the receipts completely, legibly, and unaltered. The user is supported in this by the Yokoy Mobile App, which preselects the photographic recording with a contour recognition of the receipt. This is to ensure the complete capture of the receipt to be photographed - however, this cannot be technically guaranteed (e.g., in the case of double-sided or multi-page receipts).

On the other hand, the auditor has the duty to check the data and attached supporting documents professionally and factually and to return them to the employee in case of conspicuousness or to correct them in parts.

Use cases for corrections or a rejection of the expenditure are:

- Correction of data entry errors (e.g., by the user).
- Incorrect or unverifiable entries due to an illegible document scan.
- Incomplete or unverifiable entries due to an incomplete document scan.

9.2. Special Need for Correction

Output data cannot be changed after an output has been approved. The only exception to this rule is that a subset of fields can be edited by accountants to fix errors in already locked fields that invalidate accounting exports in relation to the law. This involves a special editing process with strict controls on which fields may be edited and by whom. Like all changes, these are logged and recorded.

After an expense has been imported into the company's accounting system, this access is also no longer available, and the expense can no longer be edited.

10. Legal Notes

In various countries, legal rules apply for digital processing of invoices and receipts. Below, the rules for the key countries, Yokoy is currently present with an office, are listed.

Disclaimer: Yokoy is not liable for correctness and validity of these requirements. It is customer's responsibility to validate current legal rules.

10.1. Austria

Summary of known topics (source: WKO AT):

- Tax law provides for a basic retention period of seven years for all records and documents.
- E-invoices entitle the holder to an input tax deduction if the authenticity of the origin, the integrity of the content and the legibility are guaranteed during the retention period.
- Incoming paper invoices can be stored electronically if the complete, orderly, identical content and true-to-script reproduction is guaranteed at all times until the expiry of the statutory retention period (audit-proof archiving).
- Outgoing invoices issued with the aid of a computer system do not have to be printed out again.
- Contracts should be kept in the original. Saving as PDF is not enough.
- Scanning and saving invoices in PDF format on a USB stick, hard drive or server is not enough for audit-proof archiving, as each individual file can be modified, deleted or its sequence changed.
- Only write-once data carriers (CD-R, DVD-R, Blue-ray) or special hard disk-based archiving software can be used for revision security. There are also service providers who offer audit-proof archiving in the cloud.
- In general, a tax consultant or specialized civil engineer should be consulted to assess whether the solution is really audit-proof.
- In addition to the technical framework conditions, a uniform procedure must be defined for all invoices and the employees must be trained accordingly. It is also essential that the documents are correctly indexed. Furthermore, an internal control system should be in place in connection with electronic archiving to ensure that only authorized persons have access, and that data can be retrieved at any time.

10.2. Germany

In Germany, the legislator prescribes procedural documentation that describes the processing, storage, and control of digital documents.

This document describes the technical handling of digital receipts according to German legislation (GOBD DE) in the Spend Management platform Yokoy. Together with a customer-specific document describing the internal input channels and processes, the legally required "fiscal procedure description" is created.

It is recommended to add this technical document as an annex to the procedure documentation to be prepared specifically for the customer.

The retention period for digital documents is 10 years for commercial books, inventories, management reports, group management reports as well as the work instructions and other organizational documents required for their comprehension, receipts for entries in the books to be kept by the merchant pursuant to section 238 (1) HGB (accounting receipts), cf. section 257 (4) in conjunction with section 257 (1) no. 1, 4 HGB, section 147 (3) in conjunction with section 147 (1) no. 1, 4 HGB, § 257 section 1 no. 1, 4 HGB, § 147 section 3 in conjunction

with. § 147 section 1 no. 1, 4, §5 AO. Retention period ends with the end of calendar year where the transaction was created.

Example: on 01 Jan 2023, all receipts from 2012 can be deleted. Receipts from e.g., 01.04.2012 must not be deleted before 01.01.2023 (and not already on 01.04.2022).

According to § 14b UStG, all invoices received must be kept for 10 years. In accordance with § 14 para. 1 p. 2 ff. UStG, the authenticity of the origin, the integrity of their content and their legibility must be ensured throughout the entire storage period and guaranteed by an internal control procedure to be set up.

The retention period for digital documents is 6 years for received commercial or business letters and reproductions of sent commercial or business letters and other documents, cf. § 257 par. 1 no. 2,3 HGB, § 147 par. 3 i.V.m. § 147 (1) nos. 2, 3, 5 AO. Commercial letters are only documents that concern a commercial transaction (section 257 (2) HGB).

The present procedural documentation ensures that the digitized documents, when made readable, correspond visually with the received commercial letters and the accounting documents and with the other documents in terms of content, are available for the duration of the retention period and can be made readable at any time within a reasonable period of time (§ 257 para. 3 HGB, § 147 para. 2 AO).

The obligation to keep records begins at the end of the calendar year in which the last entry was made in the commercial ledger, the inventory was drawn up, the commercial letter was received or dispatched, or the accounting document was created (section 257 (5) HGB, section 147 (4) AO).

This procedure description is in line with the spirit and purpose of the guideline RESISCAN - Replacing Scanning (BSI TR RESISCAN -03138), Version 1.0, 12.02.2013.

Taking into account the compliance requirements, the following criteria for regularity (cf. e.g., GoBD) result in particular with regard to the process on which this procedural documentation is based.

Nr.	Anforderung	Erläuterung
1	Nachvollziehbarkeit Nachprüfbarkeit	Die Verarbeitung der einzelnen Geschäftsvorfälle sowie das dabei angewandte Buchführungs- und Aufzeichnungsverfahren müssen nachvollziehbar sein. Geschäftsvorfälle müssen sich in ihrer Entstehung und Abwicklung lückenlos verfolgen lassen (progressive und retrograde Prüfbarkeit).
2	Einzelaufzeichnungspflicht	Das Gesetz sieht für Kassenaufzeichnungen grundsätzlich die Einzelaufzeichnungspflicht vor. Das bedeutet, dass jeder Geschäftsvorfall (z. B. jede erfasste Einnahme bzw. Ausgabe in der Kasse) einzeln aufzuzeichnen ist. Ausnahmen von diesem Grundsatz werden aus Zumutbarkeitsgründen nur in engen Grenzen, i. d. R. in Verbindung mit einer „offenen Ladenkasse“ zugelassen.
3	Vollständigkeit	Die Geschäftsvorfälle sind vollzählig und lückenlos aufzuzeichnen.
4	Richtigkeit	Geschäftsvorfälle sind in Übereinstimmung mit den tatsächlichen Verhältnissen und im Einklang mit den rechtlichen Vorschriften inhaltlich zutreffend durch Belege abzubilden.
5	Lesbarkeit	Die Wiedergabe muss mit dem Original bildlich sowie inhaltlich übereinstimmen, wenn diese lesbar gemacht wird (Sichtprüfbarkeit).
6	Maschinelle Auswertbarkeit	Ermöglichung einer mathematisch-technischen Auswertung, einer Volltextsuche oder einer Prüfung im weitesten Sinne.
7	Zeitgerechte Belegsicherung	Belege sind zeitnah einer Belegsicherung zuzuführen und gegen Verlust zu sichern. Für die Kassenführung schreibt der Gesetzgeber in § 146 Abs. 1 Satz 2 AO eine tägliche Führung der Aufzeichnungen vor.
8	Ordnung	Geschäftsvorfälle sind systematisch, übersichtlich, eindeutig und identifizierbar festzuhalten.
9	Unveränderbarkeit	Informationen, die einmal in den Verarbeitungsprozess eingeführt werden, dürfen nicht mehr unterdrückt oder ohne Kenntlichmachung überschrieben, gelöscht, geändert oder verfälscht werden, dass deren ursprünglicher Inhalt nicht mehr feststellbar ist.
10	Verfügbarkeit	Die aufbewahrungspflichtigen Daten müssen (über die Dauer der gesetzlichen Aufbewahrungsfrist) verfügbar sein und unverzüglich lesbar gemacht werden können.
11	Integrität	Unversehrtheit des Inhalts.
12	Authentizität	Echtheit der Herkunft. Ein Geschäftsvorfall ist einem Verursacher eindeutig zuzuordnen.
13	Vertraulichkeit	Der unberechtigte Zugriff. - sowohl lesend als auch schreibend - ist zu unterbinden

Figure 9: Regulatory criteria (source: BMF DE)

Within the scope of the order control, a contract is drawn up between the client and the contractor on the basis of § 11 BDSG. If subcontractors can be used contractually, an order control is carried out in advance in coordination with the company data protection officer in accordance with the provisions of Section 11 BDSG. In this context, the technical and organizational measures pursuant to the Annex to Section 9 BDSG as well as the general legal requirements are checked. In addition, the appointed company data protection officer ensures an appropriate and effective integration of the data protection officer into the company processes through the data protection organization.

Separate addendum and ISO certification for this topic exists from Yokoy.

10.3. Netherlands

Accounting in the Netherlands is ruled by certain principles.

These formulate a set of rules, which ensure that the financial statement and information is clear and concise. The information provided needs to be:

1. Understandable
2. Relevant
3. Reliable
4. Comparable

Source: <https://intercompanysolutions.com/dutch-accounting-audit-requirements/>

Mandatory records to keep:

1. stock records
2. general accounts
3. payroll accounts
4. purchase and sales records
5. credit and debit accounts
6. data that are relevant to the taxation of third parties

Source: <https://business.gov.nl/regulation/keeping-business-records/>

10.3.1. Retention Period for the Records

Business records must be kept for at least 7 years. This is the retention period. Data related to immovable property must be kept for at least 10 years. Records must also be kept for 10 years if making use of the [Union scheme, housed in the One Stop Shop](#) (in Dutch).

Source: <https://business.gov.nl/regulation/keeping-business-records/>

10.3.2. Digital retention

For computer programmes and files, the retention period also applies. Digital files accessibility and usefulness must be ensured in the event of an inspection. This also applies to the associated programmes.

Source: <https://business.gov.nl/regulation/keeping-business-records/>

10.4. Spain

Required: homologation by the Spanish Tax Agency of the product

The main regulation applicable to Certified Digitization is Order EHA/962/2007, of 10 April, which develops certain provisions on telematic invoicing and electronic conservation of invoices, contained in Royal Decree 1496/2003, of 28 November, which approves the regulation regulating invoicing obligations; and also the Resolution of 24 October 2007, of the State Tax Administration Agency, on the procedure for the approval of digitization software contemplated in Order EHA/962/2007, of 10 April 2007.

Although the Order refers to Royal Decree 1496/2003, which has already been repealed, it is still in force following the publication of Royal Decree 1619/2012, of 30 November, approving the Regulation defining invoicing obligations.

Equivalent regulations have been published in four provincial councils with tax competence, since all the regulations developed for the Common Territory (a term used in the 4 provincial administrations with their own regulatory capacity to refer to the general regulations applicable to the whole state) are replicated by each of the provincial councils, bearing in mind that cross-references to other state or regional regulations must refer to the type and number of provision and to the date of 1

The list of solutions approved by the Spanish Tax Agency is available at the official website (“*Ministerio de Hacienda*”).

Royal Decree 1619/2012, of 30 November, approving the Regulation defining invoicing obligations, has given rise to these equivalent rules in the provincial (foral) territories:

- Álava: Foral Decree 18/2013, of the Council of Deputies of 28 May.
- Guipúzcoa: Foral Decree 8/2013, of 26 February.
- Navarra: Foral Decree 23/2013, of 10 April.
- Vizcaya: Foral Decree 4/2013, of 22 January.

The provincial regulation equivalent to the Order EHA/962/2007, of 10 April is the following:

- Álava: Foral Order 121/2009 of the deputy for the Treasury, Finance and Budgets of 4 March implementing certain provisions on telematic invoicing and electronic storage of invoices contained in Foral Decree 27/2005 of 5 April regulating invoicing obligations.
- Guipúzcoa: Foral Order 865/2007 of 2 August developing certain provisions on telematic invoicing and electronic storage of invoices, contained in Foral Decree 61/2004 of 15 June regulating invoicing obligations.
- Navarra: Foral Order 228/2007, of 12 June of the Counselor of Economy and Finance, developing certain provisions on telematic invoicing and electronic conservation of invoices, contained in Foral Decree 205/2004, of 17 May, approving the Regulation on invoicing obligations, on the standardisation of digitisation software.
- Vizcaya: Foral Order 1868/2009, of 2 July, developing certain provisions on telematic invoicing and electronic conservation of invoices, contained in Foral Decree 57/2004, of 6 April, regulating invoicing obligations.

In the context of Certified Digitisation, the requirements for approval are exactly the same, although the bodies before which approval is processed are the specifics of the competent provincial Council or, where appropriate, the State Tax Administration Agency.

In this way, whatever body certifies compliance with the requirements, it allows the entity that has requested the homologation of its certified digitization system to offer it in any context so that user entities can digitize their simplified or complete paper-based invoices while maintaining the legal value of the electronic copies as equivalent to originals, being able to destroy the original paper documents.

if a developer of certified digitization software obtains approval from more than one body, that software should manage in the metadata fields included in the electronic documents resulting from digitization the approval codes granted by all the bodies. The simplest and most recommendable option is to request approval only from the State Tax Administration Agency.

However, due to the applicant perception of a strong association to a provincial territory, it may be worthwhile from a commercial point of view to announce other homologations.

10.5. Switzerland

The Swiss Code of Obligations provides for the following:

book-keeping principles.

1. The complete, truthful, and systematic recording of business transactions and facts;
2. The documentary evidence for the individual accounting transactions;

3. The clarity;
4. The appropriateness with regard to the type and size of the company;
5. The verifiability.

Art. 957a para 2 OR

Records can be held on a paper-based or electronic format. (Art. 957a para 3 CO)

The general retention period for a company's books is 10 years beginning at the end of the business year. (Art. 958f CO)

The Ordinance on Bookkeeping states that the records shall not be changeable without a trace (Art. 3)

Acceptable information carriers are:

1. unchangeable information carriers, namely paper, image carriers and unchangeable data carriers;
2. changeable information carriers, if:
 - a. technical procedures are used which guarantee the integrity of the stored information (e.g., digital signature procedures),
 - b. the time at which the information is stored is verifiable in an unforgeable manner (e.g., by means of "time stamps"),
 - c. the further regulations existing at the time of storage concerning the use of the technical procedures concerned are complied with, and
 - d. the processes and procedures for their use are defined and documented, and the corresponding auxiliary information (such as logs and log files) is also retained.