Technical and Organizational Measures

In accordance with Art. 32 GDPR Art. 32 UK GDPR and Art. 8 FADP as applicable, appropriate technical and organizational measures are taken to ensure a level of security appropriate to the risk.

Yokoy operates a spend management platform designed to provide a high level of security throughout the information processing lifecycle. In addition, Yokoy has implemented a security program and information security management system that is ISO 27001 certified by TÜV Rheinland and regularly audited. Yokoy's business processes amongst others the software development are certified to ISO 9001 by Attesta Schweizer Zertifizierungsgesellschaft AG, which has an employee directly involved in the ISO 9001 Working Group, which maintains and publishes the standard. The current certificate for the ISO certifications can be downloaded here.

This document presents the binding technical and organizational measures in connection with the commissioned data processing carried out and provides information on the applicable data protection and data security concepts at Yokoy.

Scope

The technical and organizational measures described in accordance with Art. 32 GDPR, Art. 32 UK GDPR and Art. 8 FADP apply to all Yokoy companies. These are currently Yokoy Schweiz AG, based in Zurich (Switzerland), Yokoy Deutschland GmbH based in Munich (Germany), Yokoy GmbH based in Vienna (Austria), Yokoy Netherlands B.V. based in Amsterdam (Netherlands), Yokoy Pay d.o.o based in Zagreb (Croatia), and Yokoy Ltd based in London (United Kingdom).

Versioning

Name	Date	Change
v1.0	22.5.2022	Original version.
v2.0	16.2.2023	The structure of the document has been updated. Revision and expansion of the content.
v.2.1	18.8.2023	Adaptation to the new corporate structure
V.2.2	31.1.2024	Refinement in line with the yearly contract review.

Data protection and data security concept

The specific technical and organizational measures taken in accordance with Art. 32 GDPR for commissioned data processing are described below. Yokoy complies with the obligation enshrined in the GDPR Art. 32 UK GDPR and Art. 8 FADP, as applicable to protect the processing of Personal Data through appropriate technical and organizational measures and, where possible, through anonymization or pseudonymization of Personal Data. All measures taken are taking into account the risk associated with the respective data processing and correspond to the state of the art. In particular, the effectiveness of the measures takes into account the protection objectives of confidentiality, availability, integrity, and capacity. This is supported by the integration of an information security strategy and data protection measures to safeguard data processing operations.

Definition of the terms of the security value:

- Confidentiality. Protection of data, information and programs from unauthorized access and disclosure.
- Integrity. Factual and technical accuracy and completeness of all information and data during processing.
- Availability. Information, data, applications, IT systems and IT networks are available for processing.
- Resilience. Refers to an aspect of the availability and therefore the capacity of information, data, applications, IT systems and IT networks in the event of disruptions, failures or heavy use

Confidentiality

Technical and organizational measures are taken that are suitable to ensure confidentiality. Taking into account the state of the art, the costs of implementation and the nature, scope, context, and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the following measures are taken to protect the confidentiality of Personal Data.

Access control of data processing centers

Data centers

The Yokoy spend management solution is hosted in the Google Cloud. Data centers housing Google Cloud systems and infrastructure components are subject to physical access restrictions and are equipped with 24/7 on-site security personnel, security guards, access badges, biometric identification mechanisms, physical locks, and video cameras to monitor the interior and exterior of the facility. Further details on the protective measures and security features can be found at Google Cloud data center security.

As a cloud platform, Google Cloud regularly undergoes an independent review of security, privacy, and compliance controls. Information about their certifications and compliance standards of Google Cloud can be found under: GCP Compliance.

Office building

Business premises and buildings are monitored 24 hours a day by an external service provider. Offices can only be entered with personal access badge. Visitors and guests must be registered before entering, accompanied by a Yokoy employee during their stay and escorted to the exit by a Yokoy employee.

Lockable compartments are provided to prevent theft and unauthorized access to sensitive information. All employees are responsible for the secure storage of their laptops. However, the hard disks of the laptops are encrypted.

Employees are trained on the importance of physical security, including best practices for locking doors, securely handling printed documents, and reporting suspicious activity.

Printed documents are disposed of with the help of document shredders and disposal companies.

Access control of Personal Data processing systems

Yokoy offers configurable settings to ensure that Customers' data is secured, used, and accessed according to their individual requirements. With this in mind, Yokoy supports Single Sign-On (SSO) with the OpenID Connect (OIDC) and SAML 2.0 protocols, allowing Customers to use their own Identity Provider (IdP) and utilize Multi-Factor Authentication (MFA).

Yokoy employee access is governed by the company's identity provider, which enforces strict password policies and multi-factor authentication. In addition, policies are in place to meet identity lifecycle management requirements, including access provisioning, deprovisioning, authentication, authorization, and regular access reviews.

Access control for Personal Data in data processing systems

Multiple user roles are available, with different levels of access for different tasks within the review, approval, and billing processes. Customers can customize user profiles, with the ability to control access to functions, visibility/changeability of data (i.e. read, write, or read and write), type of data (invoices, expense reports and/or expenses), user groups (administrative units/departments), etc.

Access by Yokoy employees is strictly controlled. Every Yokoy employee signs a confidentiality agreement before starting work and is trained in data security. Yokoy applies the following principles:

- Awareness required. Access is granted solely on the basis of what an employee needs to carry out their work.

- Lowest authorization. The minimum access right is taken into account and assigned for each defined access.
- Segregation of duties (also known as conflict of interest). Access requests are subject to a "four-eyes check" and control.

Requests for additional access follow a formal process that includes a request and approval from a data or system owner, manager or other executive as required by Yokoy's security policies. Beyond that, no permanent access to Yokoy's production environment is granted.

Separation control

In view of the multi-client nature of Yokoy's offerings, data separation measures have been fully implemented. This includes the logical separation of clients within the application as well as the separation of development, test, and production environments.

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

Integrity

The following controls ensure the integrity of Personal Data.

Transmission control

All data is encrypted before transmission and decrypted and verified on arrival to ensure it is protected from unauthorized access or theft. The Advanced Encryption Standard (AES-256) is used, and each encryption key is itself encrypted with a regularly rotating set of master keys.

Input control

Yokoy has a process in place that checks all entered data for accuracy, completeness, and consistency. There are checks to ensure that the data entered is in the correct format and does not contain any malicious or invalid characters.

There is an audit function that records all data changes, including who made the changes and when. The cloud audit logs are stored in a highly protected repository, resulting in a secure, immutable, and highly durable audit trail.

Availability and reliability

Yokoy uses a serverless architecture where all backend services are scaled on demand. The database is automatically backed up in a separate (encrypted) cloud storage container with a retention period of 1 month and a daily backup frequency. The data recovery routines are tested regularly. Yokoy carries out continuous capacity planning and monitoring.

Availability control

Yokoy has a Business Continuity Plan (BCP) that complies with the ISO 27001 standard and describes the safety precautions and measures in place in the event of a prolonged service outage due to factors beyond its control (e.g. natural disasters, man-made events), with the aim of restoring services in the shortest possible time. The plan is reviewed every six months and tested annually.

Yokoy works with GCP as a cloud provider to store data. The database runs in high availability mode (setting for multiple availability zones) to improve durability and availability. In the event of a disaster, Yokoy relies on the automatic backups and database snapshots performed and regularly tested by GCP.

Regular review, assessment, and evaluation

Yokoy has established a data protection framework and processes to ensure appropriate monitoring, assessment, and evaluation of data protection.

Data protection management

Yokoy has appointed a full-time in-house Privacy Officer who specializes in technology law, holds an LL.M. in Law and Technology from the University of California, Berkeley, and is certified by the International Association of Privacy Professionals in EU and US law (CIPP/E and CIPP/US, respectively).

Customers sign a Data Processing Addendum as an Appendix to their SaaS Agreement. Data Processing Agreements are also in place for our Sub-Processors, and Yokoy aims to use Sub-Processors that store data exclusively in the EU or make their usage optional where possible. Where necessary, a data transfer impact assessment has been conducted.

A data transfer impact assessment has been carried out and developments in the area of data transfer are closely monitored in particular but not limited to the developments in the United States. The applicable data transfer mechanism is outlined transparently for every Sub-Processor in Appendix 3. Regular participation in online and offline events and subscriptions to relevant data protection newsletters ensure that Yokoy maintains an overview of this highly dynamic area of law.

You can find a comprehensive overview of the corresponding data protection and data security documentation here.

Incident response management

The operational availability of the software is checked regularly, and a business continuity plan is in place. Appropriate reporting channels are defined and responsibilities are defined in order to be able to respond effectively and promptly to incidents if necessary. The following measures have been taken for this purpose:

- Employees are trained accordingly.
- Reporting points and channels for (security-related) incidents have been defined.

- An organized approach was chosen.
- The documentation is retained and curated.

The experience and knowledge gained flow into the further design and improvement of the processes. The software development process is in scope of our ISO 9001 quality management system.

Order control

Measures have been taken to ensure that Personal Data processed on behalf of a Customer can only be processed in accordance with the Customer's instructions. This is described in detail in an Data Processing Agreement and signed jointly by Yokoy and the Customer as part of the Software-as-a-Service Agreement (Appendix 1).

Privacy-friendly default settings

Data protection by design

Personal Data is only collected if this is absolutely necessary (stated purpose). The categories of data processed are outlined transparently in Appendix 2 of the SaaS Agreement separated by module.

Company data is strictly separated, and users access it via their own client.

Default settings ensure that Personal Data is only processed in accordance with the respective processing purpose. Thanks to the continuous awareness-raising and training process as part of data protection management, employees are careful when handling Personal Data and consider the data protection principle of data minimization as part of the development of technical and business processes.