Technical and Organizational Measures

According to Art. 32 GDPR[1] and Art. 8 FADP[2], appropriate technical and organizational measures shall be implemented to ensure a level of security adequate to the risk.

Yokoy operates a spend management platform that has been designed to provide strong security throughout the entire information processing lifecycle. Furthermore, Yokoy has established a security program and information security management system that is ISO 27001 certified by TÜV Rheinland and reviewed periodically. The latest certificate can be provided upon request.

This document outlines the binding technical and organizational measures associated with commissioned data processing operations carried out and provides information about the valid data protection and data backup concepts at Yokoy.

Scope

The technical and organizational measures. according to Art. 32 EU GDPR described apply to all Yokoy entities. Those are currently Yokoy Switzerland Ltd registered in Zurich, Yokoy Deutschland GmbH registered in Munich (Germany), Yokoy GmbH registered in Vienna (Austria), and Yokoy Netherlands B.V. registered in Amsterdam (the Netherlands).

Change History

Name	Date	Change
v1.0	22.5.2022	Initial version
v2.0	16.2.2023	Updated document structure, as well as revised and expanded its content
v.2.1	9.8.2023	Reflecting the new legal structure of the company.

Data Protection and Data Security Concept

The following outlines the specific technical and organizational measures implemented pursuant to Art. 32 EU General Data Protection Regulation (GDPR) for commissioned data processing. Yokoy fulfills the obligation established in the GDPR to safeguard processing of personal data by means of appropriate technical and organizational measures and, where possible, anonymising or pseudonymising personal data. All measures implemented must take the risk associated with the respective data processing operation into consideration and be state of the art. In particular, the effectiveness of the measure should take account of the protection objectives of

[1] Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
[2] Federal Act on Data Protection entering into force on September 1st 2023.

confidentiality, availability, integrity and capacity. This is supported by integrating an information security strategy and data protection measures to safeguard data processing operations.

Definition of security value terms:

- Confidentiality. Protection of data, information and programmes against 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. Denoted as an aspect of availability and thus the capacity of information, data, applications, IT systems and IT networks in the event of malfunction, failure or heavy use.

Confidentiality

Technical and organizational measures are implemented that are appropriate for safeguarding 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 safeguard the confidentiality of personal data.

Access Control of Data Processing Centres

Data Centres

The Yokoy spend management solution is hosted in Google Cloud. Data centers that house Google Cloud systems and infrastructure components are subject to physical access restrictions and equipped with 24x7 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. More details on their safeguards and security features can be found at: GCP Data Center Security.

As a Cloud Platform, Google Cloud regularly undergoes independent verification of security, privacy, and compliance controls. Information about their certifications and compliance standards can be found at: GCP Compliance.

Office Buildings

Business premises and buildings are monitored 24 hours a day by an external property provider. Offices can be entered with personal access keys only. 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 storage is available to prevent theft and unauthorized access to sensitive information. All employees are responsible for storing their laptops safely. Nevertheless, laptops' hard-drives are encrypted.

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

Printed documents are disposed of by means of document shredders and disposal firms.

Access Control of Data Processing Systems

Yokoy offers configurable settings to help ensure that customers' data is secured, used, and accessed according to their unique requirements. To this extent, Yokoy fully supports Single Sign-On (SSO) using both OpenID Connect (OIDC) and SAML 2.0 protocols, allowing customers to use their own Identity Provider (IdP) and leverage Multi-Factor Authentication (MFA).

Access by the Yokoy workforce is ruled by the corporate Identity Provider, with a strict password policy and Multi-Factor Authentication enforcement. In addition, policies are in place that address requirements for identity lifecycle management including access provisioning, deprovisioning, authentication, authorisation, and periodic access reviews.

Access Control of Personal Data in Data Processing Systems

Several user access roles are available, with different access-levels for different tasks within the review, approval, and settlement processes. 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), among others.

Access by the Yokoy workforce is heavily controlled. Every Yokoy employee signs a non-disclosure agreement prior to the start of employment, and gets trained in data security. In addition, measures are implemented that deny unauthorized personnel access to data processing systems that process and/or use personal data. This is done by implementing the following principles:

- Need-to-know. Access is given strictly based on what an employee requires to perform his or her job.
- Least privilege. The minimum access privilege is considered and assigned for any access that is defined.
- Segregation of duties (also known as conflict of interest). Access requests are subject to a "four eyes" review and control.

Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Yokoy's security policies. In addition, no permanent access is given to the Yokoy production environment.

Separation Control

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 as well as the separation of development, testing and production environments.

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

Integrity

The following checks ensure the integrity of personal data.

Transfer Control

All data is encrypted before transmission and decrypted and verified on arrival, to ensure that 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 rotated set of master keys.

Input Control

Yokoy validates all input data for accuracy, completeness, and consistency. Controls are in place to ensure that the data entered is in the correct format and does not contain any malicious or invalid characters.

An audit function is in place, recording all changes made to data, including who made the changes and when. Cloud audit logs reside in highly protected storage, resulting in a secure, immutable, and highly durable audit trail.

Availability and Resilience

Yokoy guarantees that personal data is protected against the risk of accidental destruction or loss. Yokoy uses a "serverless architecture" where all used services scale on demand. The database is automatically backed up to a separate (encrypted) cloud storage bucket with a retention policy of 1 Month with a daily backup frequency. The data backup is protected against unauthorized access. The Data recovery routines are regularly tested.

Day-to-day operations are secured by ongoing capacity planning and monitoring.

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.

Regular Review, Assessment and Evaluation

Yokoy has established a data protection framework and set up related processes to ensure adequate monitoring, assessment and evaluation related to data protection.

Data Protection Management

Yokoy has appointed an internal full time Data Protection Officer who is specialized in technology law with an LL.M. in Law and Technology from the University of California, Berkeley and certified by the International Association of Privacy Professionals in EU and US law (CIPP/E and CIPP/US respectively).

A publicly available privacy policy and cookie policy inform about Yokoy's approach to Privacy whereas the customers sign a Data Processing Addendum as an Annex to their SaaS Agreement. Data Processing Addendums are also in

place for our Sub Processors whereas we strive to use Subprocessors who store data exclusively in the EU where possible.

A transfer Impact Assessment is in place and the developments on the transferring of data is closely watched. By attending regular on- and offline events and subscriptions to relevant privacy newsletters it is ensured Yokoy keeps track of this highly dynamic field of law.

Incident Response Management

The operational availability of the software is regularly checked and a Business Continuity Plan is in place. Relevant reporting channels are defined and responsibilities established to be able to respond to incidents in an effective and timely manner, if necessary. To this end, the following measures have been implemented:

- Employees are trained accordingly.
- Reporting points and channels have been defined for (security-related) incidents.
- An organized approach has been adopted.
- Documentation is maintained.

Experience gained is channeled into the further design and improvement of processes.

Order Control

Measures have been implemented to ensure that personal data processed on behalf of a customer can only be processed in accordance with the instructions of the customer. This is thoroughly described in a Data Processing Addendum and mutually signed by Yokoy and the customer as part of the Software as a Service Agreement.

Privacy Friendly Preferences

Privacy by Design

Personally identifiable data is only collected when absolutely necessary (purpose stated). This includes, employee name, email, main cost center, legal entity (required to assign expenses) as well as expense claims & receipts.

Company data is strictly separated, user access is granted through a dedicated tenant.

Default settings ensure that personal data are only processed in accordance with the specific processing purpose. Thanks to the ongoing awareness and training process within the context of data protection management, employees are careful when handling personal data and consider the privacy principle of data minimisation to be part of the development of technical and business processes.