Technical and Organizational Measures

1. Introduction

This document outlines the Technical and Organizational Measures (TOMs) Yokoy has taken to protect your data from unauthorized access, misuse, accidental deletion and loss. It represents binding technical and organizational measures in connection with the commissioned data processing and provides information on the applicable data protection and data security concepts at Yokoy.

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 27001:2013 certified by TÜV Rheinland and regularly audited. Yokoy's business processes, such as others the software development processes, are certified to ISO 9001:2015 by Attesta Schweizer Zertifizierungsgesellschaft AG. The current certificates for the ISO certifications can be downloaded here.

Further, Yokoy is certified according to the PCI-DSS 4.0 (Payment Card Industry-Data Security Standard). The certification was issued by PGI (Protection Group International). The relevant certificate can be downloaded here.

2. 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 as outlined in Imprint of our website.

3. 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.
V.2.3	16.9.2024	Information added on our PCI-DSS certification and our Parkerian Hexad model.

4. Data protection and data security concept

Yokoy guides its security efforts via the Parkerian Hexad model. This is a comprehensive security framework that expands on the traditional CIA (Confidentiality, Integrity, Availability) triad by including three additional critical elements: Possession/Control, Authenticity, and Utility. Yokoy's approach to security embraces this model to ensure holistic protection of client data. By safeguarding not only the confidentiality, integrity, and availability of information but also ensuring that data remains under authorized control, is genuine and unaltered, and remains useful and accessible, we provide a robust defense against a wide array of potential threats. This multifaceted approach allows us to address complex security challenges and deliver resilient, reliable solutions for our clients.

All measures taken consider the risk associated with the respective data processing and correspond to the state of the art. In particular, the effectiveness of the measures considers the protection objectives as described below. This is supported by the integration of an information security strategy and data protection measures to safeguard data processing operations.

5. 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.
- Possession/Control. The principle of ensuring that only those with the appropriate authority can access and control information and systems. This can be done through access controls such as user authentication and authorization.
- Authenticity. The principle of ensuring that data and transactions are from their claimed source. This can be done through encryption, digital signatures, and other methods to ensure data is from the intended source.
- Utility. The principle of ensuring that information is useful and understandable. For example, otherwise secure information, if encrypted with a lost decryption key would not be said to have utility.

These attributes of information are atomic in that they are not broken down into further constituents; they are non-overlapping in that they refer to unique aspects of information. Any information security breach can be described as affecting one or more of these fundamental attributes of information.

6. Confidentiality

Technical and organizational measures are taken that are suitable to ensure confidentiality. Considering 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.

6.1. Access control of data processing centers (Possession/Control)

6.1.1. Data centers

The Yokoy spend management solution is hosted in Google's Cloud Platform (GCP). 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.

6.1.2. Office building

Business premises and buildings are monitored 24 hours a day by an external service provider. Offices can only be entered with a 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 in 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.

6.2. Access control of Personal Data processing systems (possession/control)

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.

6.2.1. For Customers

User roles
Multiple user roles are available, with distinct 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.

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.

6.2.2. For Yokoy employees

Access by Yokoy employees is strictly controlled. Every Yokoy employee signs a confidentiality agreement before starting work and is trained and tested 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-eye 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.

7. Integrity

The following controls ensure the integrity of Personal Data.

7.1. Transmission control (authenticity)

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 encrypted with a regularly rotating set of master keys.

7.2. Input control (integrity and utility)

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.

8. 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.

8.1. 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, human-caused events), with the aim of restoring services in the shortest possible time. The plan is reviewed every six months and tested annually.

8.2. Reliability

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.

9. Regular review, assessment, and evaluation

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

10. 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) as well as AIGP (AI Governance Professional) also issued by the IAPP.

Customers sign a Data Processing Addendum as an Appendix to the 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. Should transfers to third-countries be necessary transfer mechanisms according to chapter V of the GDPR are in place.

A data transfer impact assessment has been carried out and developments in 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 to the SaaS Agreement. 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.

The DPO is supported by a dedicated security team who is responsible for the technical side of data protection.

11. 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.

12. Instruction 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 a Data Processing Addendum and signed jointly by Yokoy and the Customer as part of the Agreement.

13. Data Protection by Design and by default

13.1. 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 to the SaaS Agreement separated by the respective Yokoy Packages.

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

13.2. Data protection by default

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. All employees are bound by confidentiality agreements by virtue of their working contract and an additional confidentiality agreement specifically focusing on data protection.