yokoy

Technische und organisatorische Maßnahmen (TOMs)

1. Einleitung

Dieses Dokument beschreibt die technischen und organisatorischen Maßnahmen (TOMs), die Yokoy getroffen hat, um Ihre Daten vor unberechtigtem Zugriff, Missbrauch, versehentlicher Löschung und Verlust zu schützen. Es handelt sich hierbei um verbindliche technische und organisatorische Maßnahmen im Zusammenhang mit der Auftragsdatenverarbeitung und soll Auskunft über die bei Yokoy geltenden Datenschutz- und Datensicherheitskonzepte geben.

Yokoy betreibt eine Ausgabenmanagementplattform, die darauf ausgelegt ist, ein hohes Maß an Sicherheit während des gesamten Lebenszyklus der Informationsverarbeitung zu gewährleisten. Darüber hinaus hat Yokoy ein Sicherheitsprogramm und ein Managementsystem für Informationssicherheit eingeführt, das vom TÜV Rheinland nach ISO 27001:2013 zertifiziert ist und regelmäßig überprüft wird. Die Geschäftsprozesse von Yokoy, wie insbesondere jener für die Software-Entwicklung, sind nach ISO 9001:2015 durch die Attesta Schweizer Zertifizierungsgesellschaft AG zertifiziert. Die aktuellen Zertifikate für die ISO-Zertifizierungen können hier heruntergeladen werden.

Yokoy ist zudem nach dem PCI-DSS 4.0 (Payment Card Industry-Data Security Standard) Standard zertifiziert. Die Zertifizierung erfolgte durch PGI (Protection Group International).

2. Scope

Die beschriebenen technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO, Art. 32 UK-GDPR und Art. 8 DSG gelten für alle im Impressum unserer Webseite gelisteten Yokoy-Gesellschaften

3. Versionen

Name	Datum	Änderungen
v1.0	22.5.2022	Originalfassung.
v2.0	16.2.2023	Die Struktur des Dokuments wurde aktualisiert. Überarbeitung und Erweiterung des Inhalts.
v.2.1	18.8.2023	Anpassung an die neue Unternehmensstruktur
V.2.2	31.1.2024	Verfeinerung im Einklang mit der jährlichen Vertragsüberprüfung

V.2.3	16.9.2024	Ergänzung betreffend der erworbenen PCI-DSS 4.0 Zertifizierung und dem Datensicherheitskonzept der Parkerschen Hexade.

4. Datenschutz und Datensicherheitskonzept

Yokoy's Datensicherheitskonzept entspricht dem Parkerschen Hexad-Modell. Dabei handelt es sich um ein umfassendes Sicherheitskonzept, welches die traditionelle CIA-Triade (Vertraulichkeit, Integrität, Verfügbarkeit) um drei zusätzliche kritische Elemente erweitert: Besitz/Kontrolle, Authentizität und Nützlichkeit. Der Sicherheitsansatz von Yokoy bedient sich dieses Modells, um einen ganzheitlichen Schutz der Kundendaten zu gewährleisten. Indem Yokoy nicht nur die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sicherstellt, sondern auch dafür sorgt, dass die Daten unter autorisierter Kontrolle, echt, unverändert, nützlich und zugänglich bleiben, bietet Yokoy eine robuste Verteidigung gegen eine breite Palette potenzieller Bedrohungen. Dank dieses vielschichtigen Ansatzes kann Yokoy komplexe Sicherheitsherausforderungen bewältigen und unseren Kunden belastbare, zuverlässige Lösungen bieten.

Alle getroffenen Massnahmen tragen dem mit der jeweiligen Datenverarbeitung verbundenen Risiko Rechnung und entsprechen dem neusten Stand der Technik. Bei der Wirksamkeit der Maßnahmen werden insbesondere die unten beschriebenen Schutzziele berücksichtigt. Unterstützt wird die Erreichung dieser Ziele durch die Integration einer Informationssicherheitsstrategie und von Datenschutzmassnahmen zur Absicherung der Datenverarbeitungsvorgänge.

5. Schutzziele

- Vertraulichkeit: Schutz von Daten, Informationen und Programmen vor unberechtigtem Zugriff und Offenlegung.
- Integrität: Sachliche und technische Richtigkeit und Vollständigkeit aller Informationen und Daten bei der Verarbeitung.
- Verfügbarkeit: Informationen, Daten, Anwendungen, IT-Systeme und IT-Netzwerke sind für die Verarbeitung verfügbar.

- Besitz/Kontrolle: Dieses Prinzip stellt sicher, dass nur diejenigen, die über die entsprechenden Befugnisse verfügen, auf Informationen und Systeme zugreifen und diese kontrollieren können. Dies kann durch Zugangskontrollen wie Benutzerauthentifizierung und -autorisierung erreicht werden.
- Authentizität: Dieses Prinzip stellt sicher, dass Daten und Transaktionen von der angegebenen Quelle stammen. Dies kann durch Verschlüsselung, digitale Signaturen und andere Methoden erreicht werden, die sicherstellen, dass die Daten aus der vorgesehenen Quelle stammen.

- Nützlichkeit: Dieses Prinzip stellt sicher, dass Informationen nützlich und verständlich sind. Zum Beispiel würden ansonsten sichere Informationen, die mit einem verlorenen Entschlüsselungscode verschlüsselt sind, keinen Nutzen haben.

Diese Schutzziele und Attribute von Informationen sind so detailliert, dass sie nicht in weitere Bestandteile aufgeschlüsselt werden können; sie sind nicht überlappend, da sie sich auf eindeutige Aspekte von Informationen beziehen. Jede Verletzung der Informationssicherheit kann als Beeinträchtigung eines oder mehrerer dieser grundlegenden Sicherheitsziele und Attribute von Informationen beschrieben werden.

6. Vertraulichkeit

Es werden technische und organisatorische Maßnahmen getroffen, die geeignet sind, die Vertraulichkeit zu gewährleisten. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, des Kontextes und der Zwecke der Verarbeitung sowie des Risikos unterschiedlicher Eintrittswahrscheinlichkeit und Schwere für die Rechte und Freiheiten natürlicher Personen werden folgende Maßnahmen zum Schutz der Vertraulichkeit der personenbezogenen Daten von ergriffen.

6.1. Zugangskontrolle (Besitz / Kontrolle)

6.1.1. Datenzentren

Die Ausgabenmanagementlösung Yokoy wird in der Google Cloud Platform (GCP) gehostet. Rechenzentren, in denen Systeme und Infrastrukturkomponenten der Google Cloud untergebracht sind, unterliegen physischen Zugangsbeschränkungen und sind mit Sicherheitspersonal rund um die Uhr vor Ort, Sicherheitspersonal, Zugangsausweisen, biometrischen Identifizierungsmechanismen, physischen Schlössern und Videokameras zur Überwachung des Innen- und Außenbereichs der Einrichtung ausgestattet. Weitere Einzelheiten zu den Schutzmaßnahmen und Sicherheitsmerkmalen sind unter Sicherheit im Google Cloud-Rechenzentrum zu finden.

Als Cloud-Plattform unterzieht sich Google Cloud regelmäßig einer unabhängigen Überprüfung von Sicherheit, Datenschutz und Compliance-Kontrollen. Informationen über die Zertifizierungen und Compliance-Standards von Google Cloud finden Sie unter: GCP-Compliance.

6.1.2. Bürogebäude

Geschäftsräume und Gebäude werden 24 Stunden am Tag von einem externen Dienstleister überwacht. Büros können nur mit einem persönlichen Badge betreten werden. Besucher und Gäste müssen vor dem Betreten registriert werden, während ihres Aufenthalts von einem Yokoy-Mitarbeitenden begleitet und von einem Yokoy-Mitarbeitenden zum Ausgang begleitet werden.

Es sind abschließbare Fächer vorhanden, um Diebstahl und unbefugten Zugriff auf sensible Informationen zu verhindern. Alle Mitarbeitenden sind für die sichere Aufbewahrung ihrer Laptops

verantwortlich. Die Festplatten der Laptops sind verschlüsselt, um im Falle eines Diebstahls oder Verlusts des Laptops den Zugriff auf Daten zu verunmöglichen.

Die Mitarbeitenden werden über die Bedeutung der physischen Sicherheit geschult, einschließlich der Best Practices für das Verschließen von Türen, den sicheren Umgang mit gedruckten Dokumenten und das Melden verdächtiger Aktivitäten.

Gedruckte Dokumente werden mit Hilfe von Aktenvernichtern und Entsorgungsunternehmen entsorgt.

6.2. Systeme zur Verarbeitung Personenbezogener Daten

Yokoy bietet konfigurierbare Einstellungen, um sicherzustellen, dass die Daten der Kunden gesichert, genutzt und entsprechend ihren individuellen Anforderungen abgerufen werden. Zu diesem Zweck unterstützt Yokoy Single Sign-On (SSO) mit den Protokollen OpenID Connect (OIDC) und SAML 2.0, so dass Kunden ihren eigenen Identity Provider (IdP) verwenden und die Multi-Faktor-Authentifizierung (MFA) nutzen können.

Der Zugang der Yokoy-Mitarbeitenden wird durch den Identitätsanbieter des Unternehmens geregelt, der strenge Passwortrichtlinien und eine Multi-Faktor-Authentifizierung durchsetzt. Darüber hinaus gibt es Richtlinien, um die Anforderungen des Identitätslebenszyklusmanagements zu erfüllen, einschließlich Zugriffsbereitstellung, Deprovisionierung, Authentifizierung, Autorisierung und regelmäßige Zugriffsüberprüfungen.

6.2.1. Für Kunden

Benutzerrollen (Besitz/Kontrolle)
Es stehen mehrere Benutzerrollen zur Verfügung, mit unterschiedlichen Zugriffsebenen für verschiedene Aufgaben innerhalb der Überprüfungs-, Genehmigungs- und Abrechnungsprozesse. Die Kunden können die Benutzerprofile anpassen und den Zugriff auf Funktionen, die Sichtbarkeit/Änderbarkeit von Daten (d. h. Lesen, Schreiben oder Lesen und Schreiben), die Art der Daten (Rechnungen, Spesenabrechnungen und/oder Ausgaben), Benutzergruppen (Verwaltungseinheiten/Abteilungen) usw. steuern.

Kontrolle der Datentrennung (Besitz/Kontrolle)
Angesichts des mandantenfähigen Charakters der Angebote von Yokoy wurden Maßnahmen zur Datentrennung vollständig umgesetzt. Dazu gehören die logische Trennung von Clients innerhalb der Anwendung sowie die Trennung von Entwicklungs-, Test- und Produktionsumgebungen. Darüber hinaus wird der Zugriff auf die Anwendungsdaten mit Hilfe von rollenbasierten Zugriffskontrollen (Role Based Access Controls, RBAC) gesteuert, so dass nur autorisierte Benutzer logischerweise auf die vorgesehenen Daten zugreifen können.

6.2.2. Für Yokoy-Mitarbeitende

Der Zugang von Yokoy-Mitarbeitenden wird streng kontrolliert. Jeder Yokoy-Mitarbeitende unterschreibt vor Arbeitsbeginn eine Vertraulichkeitsvereinbarung und wird in Sachen Datensicherheit geschult und geprüft. Yokoy wendet die folgenden Grundsätze an:

- Zugang nur soweit erforderlich. Der Zugang wird ausschließlich auf der Grundlage dessen gewährt, was ein Mitarbeiter für die Ausführung seiner Arbeit benötigt.
- Geringste Berechtigung. Das Mindestzugriffsrecht wird berücksichtigt und für jeden definierten Zugriff zugewiesen.
- Aufgabentrennung (auch bekannt als Interessenkonflikt). Zugangsanträge unterliegen einer "Vier-Augen-Prüfung" und Kontrolle.

Anträge auf zusätzlichen Zugang folgen einem formalen Prozess, der einen Antrag und die Genehmigung eines Daten- oder Systemeigentümers, Managers oder einer anderen Führungskraft gemäß den Sicherheitsrichtlinien von Yokoy umfasst. Darüber hinaus wird kein permanenter Zugriff auf die Produktionsumgebung von Yokoy gewährt.

7. Integrität

Die folgenden Kontrollen gewährleisten die Integrität der personenbezogenen Daten.

7.1. Kontrolle der Übertragung (Authentizität)

Alle Daten werden vor der Übertragung verschlüsselt und bei der Ankunft entschlüsselt und überprüft, um sicherzustellen, dass sie vor unbefugtem Zugriff oder Diebstahl geschützt sind. Der Advanced Encryption Standard (AES-256) wird verwendet, und jeder Verschlüsselungsschlüssel wird selbst mit einem regelmäßig wechselnden Satz von Hauptschlüsseln verschlüsselt.

7.2. Eingabekontrolle (Integrität und Nützlichkeit)

Yokoy verfügt über einen Prozess, der alle eingegebenen Daten auf Richtigkeit, Vollständigkeit und Konsistenz überprüft. Es wird geprüft, ob die eingegebenen Daten das richtige Format haben und keine bösartigen oder ungültigen Zeichen enthalten.

Es gibt eine Audit-Funktion, die alle Datenänderungen aufzeichnet, einschließlich der Angabe, wer die Änderungen wann vorgenommen hat. Die Cloud-Audit-Protokolle werden in einem hochgradig geschützten Repository gespeichert, was zu einem sicheren, unveränderlichen und äußerst dauerhaften Audit-Trail führt.

8. Verfügbarkeit und Zuverlässigkeit

Yokoy verwendet eine serverlose Architektur, bei der alle Backend-Dienste nach Bedarf skaliert werden. Die Datenbank wird automatisch in einem separaten (verschlüsselten) Cloud-

Speichercontainer mit einer Aufbewahrungsfrist von einem Monat und einer täglichen Sicherungsfrequenz gesichert. Die Datenwiederherstellungsroutinen werden regelmäßig getestet. Yokoy führt eine kontinuierliche Kapazitätsplanung und -überwachung durch.

8.1. Verfügbarkeitskontrolle

Yokoy verfügt über einen Business Continuity Plan (BCP), der der Norm ISO 27001 entspricht und die Sicherheitsvorkehrungen und -maßnahmen für den Fall eines längeren Ausfalls von Diensten aufgrund von Faktoren, die sich der Kontrolle des Unternehmens entziehen (z. B. Naturkatastrophen, von Menschen verursachte Ereignisse), beschreibt, mit dem Ziel, die Dienste so schnell wie möglich wiederherzustellen. Der Plan wird alle sechs Monate überprüft und jährlich getestet.

8.2. Zuverlässigkeit

Yokoy arbeitet mit Google Cloud Platform (GCP) als Cloud-Anbieter, um Daten zu speichern. Die Datenbank läuft im Hochverfügbarkeitsmodus (Einstellung für mehrere Verfügbarkeitszonen), um die Haltbarkeit und Verfügbarkeit zu verbessern. Im Falle einer Katastrophe verlässt sich Yokoy auf die automatischen Backups und Datenbank-Snapshots, die von GCP durchgeführt und regelmäßig getestet werden.

9. Regelmäßige Überprüfung, Bewertung und Evaluierung

Yokoy hat Prozesse eingerichtet, um eine angemessene Überwachung, Bewertung und Evaluierung des Datenschutzes und der Datensicherheit zu gewährleisten.

10. Datenschutz

Yokoy hat einen internen Datenschutzbeauftragten ernannt, der auf Technologierecht spezialisiert ist, einen LL.M. in Recht und Technologie von der University of California, Berkeley, besitzt und von der International Association of Privacy Professionals in EU- und US-Recht (CIPP/E bzw. CIPP/US) sowie KI-Recht (AIGP) zertifiziert ist.

Kunden unterzeichnen einen Auftragsverarbeitungsvertrag (AVV) als Anhang zum SaaS-Vertrag. Für unsere Unterauftragsverarbeiter gelten ebenfalls Vereinbarungen zur Datenverarbeitung, und Yokoy ist bestrebt, Unterauftragsverarbeiter zu verwenden, die Daten ausschließlich in der EU speichern oder deren Nutzung optional ist, sofern dies operationell möglich ist. Soweit erforderlich, wurde eine Folgenabschätzung für den Datentransfer durchgeführt und entsprechende.

Es wurde eine Folgenabschätzung für die Datenübermittlungen in Drittstaaten durchgeführt. Aktuelle Entwicklungen im Bereich der Datenübermittlung werden genau verfolgt, insbesondere, aber nicht ausschließlich, die Entwicklungen in den Vereinigten Staaten. Der anwendbare Datenübermittlungsmechanismus ist für jeden Unterauftragsverarbeiter in Anhang 3 des SaaS-Vertrags transparent dargestellt. Die regelmäßige Teilnahme an Online- und Offline-

Veranstaltungen und das Abonnement einschlägiger Datenschutz-Newsletter sorgen dafür, dass Yokoy den Überblick über dieses äußerst dynamische Rechtsgebiet behält.

Einen umfassenden Überblick über die entsprechenden Datenschutz- und Datensicherheitsdokumente finden Sie finden Sie hier.

Der Datenschutzbeauftragte wird durch das hauseigene Security Team unterstützt, um die technische Seite des Datenschutzes zu gewährleisten.

11. Incident Response Management

Die betriebliche Verfügbarkeit der Software wird regelmäßig überprüft und es gibt einen Plan zur Aufrechterhaltung des Betriebs. Es werden geeignete Meldekanäle eingerichtet und Zuständigkeiten festgelegt, um im Bedarfsfall wirksam und zeitnah auf Vorfälle reagieren zu können. Zu diesem Zweck wurden die folgenden Maßnahmen ergriffen:

- Die Mitarbeiter werden entsprechend geschult.
- Es wurden Meldestellen und -kanäle für (sicherheitsrelevante) Vorfälle festgelegt.
- Es wurde ein organisierter Ansatz gewählt.
- Die Dokumentation wird aufbewahrt und gepflegt.

Die gewonnenen Erfahrungen und Erkenntnisse fließen in die weitere Gestaltung und Verbesserung der Prozesse ein. Der Prozess der Entwicklung ist zudem nach den Vorgaben von ISO 9001 zertifiziert.

12. Weisungskontrolle

Es wurden Maßnahmen ergriffen, um sicherzustellen, dass Personenbezogene Daten, die im Auftrag eines Kunden verarbeitet werden, nur in Übereinstimmung mit den Weisungen des Kunden verarbeitet werden können. Dies ist in einem AVV detailliert beschrieben und gemeinsam von Yokoy und dem Kunden als Teil des Software-as-a-Service Agreement unterzeichnet (Anhang 1).

13. Datenschutz durch Technikgestaltung und Datenschutzfreundliche Voreinstellungen

13.1. Datenschutz durch Technikgestaltung

Personenbezogene Daten werden nur erhoben, wenn dies absolut notwendig ist (angegebener Zweck). Die verarbeiteten Datenkategorien sind in Anhang 2 des SaaS-Vertrags nach Modulen getrennt transparent dargestellt.

Die Unternehmensdaten sind strikt getrennt, und die Nutzer greifen über ihren eigenen Client darauf zu.

13.2. Datenschutzfreundliche Voreinstellungen

Standardeinstellungen stellen sicher, dass personenbezogene Daten nur gemäß dem jeweiligen Verarbeitungszweck verarbeitet werden. Dank des kontinuierlichen Sensibilisierungs- und Schulungsprozesses im Rahmen des Datenschutzmanagements gehen Mitarbeitende sorgfältig mit Personenbezogenen Daten um und berücksichtigen das Datenschutzprinzip der Datenminimierung bei der Entwicklung von technischen und geschäftlichen Prozessen.

Alle Mitarbeiter sind durch ihren Arbeitsvertrag und eine zusätzliche, speziell auf den Datenschutz ausgerichtete Vertraulichkeitsvereinbarung gebunden.