Technische und organisatorische Massnahmen (TOMs)

Gemäss Art. 32 DS-GVO und 8 nDSG müssen geeignete technische und organisatorische Massnahmen getroffen werden, um ein dem Risiko angemessenes Sicherheitsniveau zu gewährleisten.

Yokoy betreibt eine Ausgabenmanagement-Plattform, die so konzipiert wurde, dass sie während des gesamten Lebenszyklus der Informationsverarbeitung eine hohe Sicherheit bietet. Darüber hinaus hat Yokoy ein Sicherheitsprogramm und ein Managementsystem für Informationssicherheit eingeführt, das vom TÜV Rheinland nach ISO 27001 zertifiziert ist und regelmässig überprüft wird. Das aktuelle Zertifikat kann auf Anfrage zur Verfügung gestellt werden. Die Geschäftsprozesse von Yokoy sind nach ISO 9001 zertifiziert durch die Attesta Schweizer Zertifizierungsgesellschaft AG, welche durch einen Mitarbeiter direkt Einsitz in der ISO 9001 Working Group hat, welche die Norm pflegt und herausgibt.

Dieses Dokument stellt die verbindlichen technischen und organisatorischen Massnahmen im Zusammenhang mit den durchgeführten Auftragsdatenverarbeitungen dar und informiert über die geltenden Datenschutz- und Datensicherungskonzepte bei Yokoy.

Scope

Die beschriebenen technischen und organisatorischen Massnahmen gemäss Art. 32 DS-GVO gelten für sämtliche Yokoy Gesellschaften. Dies sind derzeit die Yokoy Schweiz AG mit Sitz in Zürich, die Yokoy Deutschland GmbH mit Sitz in München (Deutschland), die Yokoy GmbH mit Sitz in Wien (Österreich) und die Yokoy Netherlands B.V. mit Sitz in Amsterdam (Niederlande).

Versionierung

Name	Datum	Änderungen
v1.0	22.5.2022	Ursprüngliche Version.
v2.0	16.2.2023	Die Struktur des Dokuments wurde aktualisiert. Überarbeitung und Erweiterung des Inhalts.
V 2.1	10.8.2023	Anpssung an neue Unternehmensstruktur

Datenschutz und Datensicherheitskonzept

Im Folgenden werden die spezifischen technischen und organisatorischen Massnahmen, die gemäss Art.

32 EU-Datenschutz-Grundverordnung (DS-GVO) für die Auftragsdatenverarbeitung getroffen wurden. Yokoy kommt der in der DS-GVO verankerten Verpflichtung nach, die Verarbeitung personenbezogener Daten durch geeignete technische und organisatorische Massnahmen und, soweit möglich, durch Anonymisierung oder Pseudonymisierung personenbezogener Daten zu schützen. Alle getroffenen Massnahmen müssen dem mit der jeweiligen Datenverarbeitung verbundenen Risiko Rechnung tragen und dem Stand der Technik entsprechen. Insbesondere soll die Wirksamkeit der Massnahmen den Schutzzielen Vertraulichkeit, Verfügbarkeit, Integrität und Kapazität Rechnung tragen. Unterstützt wird dies durch die Integration einer Informationssicherheitsstrategie und von Datenschutzmassnahmen zur Absicherung von Datenverarbeitungsvorgängen.

Definition der Begriffe des Sicherheitswertes:

- 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-Netze sind für die Verarbeitung verfügbar.
- Ausfallsicherheit. Bezeichnet einen Aspekt der Verfügbarkeit und damit der Kapazität von Informationen, Daten, Anwendungen, IT-Systemen und IT-Netzen im Falle von Störungen, Ausfällen oder starker Beanspruchung.

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 Kontexts und der Zwecke der Verarbeitung sowie der unterschiedlichen Wahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen werden die folgenden Massnahmen zum Schutz der Vertraulichkeit personenbezogener Daten getroffen.

Zugangskontrolle zu Daten-Zentren

Die Yokoy-Ausgabenmanagementlösung wird in der Google Cloud 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 Identifikationsmechanismen, physischen Schlössern und Videokameras zur Überwachung des Innen- und Aussenbereichs der Einrichtung ausgestattet. Weitere Details zu den Schutzmassnahmen und Sicherheitsmerkmalen finden Sie unter: GCP Data Center Security.

Als Cloud-Plattform unterzieht sich Google Cloud regelmässig einer unabhängigen Überprüfung der Sicherheits-, Datenschutz- und Compliance-Kontrollen. Informationen über ihre Zertifizierungen und Compliance-Standards finden Sie unter: GCP-Compliance.

Bürogebäude

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

Um Diebstahl und unbefugten Zugang zu sensiblen Informationen zu verhindern, gibt es abschliessbare Fächer. Alle Mitarbeiter sind für die sichere Aufbewahrung ihrer Laptops verantwortlich. Die Festplatten der Laptops sind jedoch verschlüsselt.

Die Mitarbeiter werden in der 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.

Zugangskontrolle von Datenverarbeitungssystemen

Yokoy bietet konfigurierbare Einstellungen, um sicherzustellen, dass die Daten der Kunden entsprechend ihren individuellen Anforderungen gesichert, genutzt und abgerufen werden. In diesem Sinne 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-Mitarbeiter wird durch den Identitätsanbieter des Unternehmens geregelt, der strenge Passwortrichtlinien und eine Multi-Faktor-Authentifizierung durchsetzt. Darüber hinaus gibt es Richtlinien, die die Anforderungen an das Identitäts-Lebenszyklus-Management erfüllen, einschliesslich Zugriffsbereitstellung, Deprovisionierung, Authentifizierung, Autorisierung und regelmässiger Zugriffsüberprüfungen.

Zugangskontrolle für personenbezogene Daten in Datenverarbeitungssystemen

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

Der Zugang der Yokoy-Mitarbeiter wird streng kontrolliert. Jeder Yokoy-Mitarbeiter unterzeichnet vor Beginn seiner Tätigkeit eine Geheimhaltungsvereinbarung und wird in Sachen Datensicherheit geschult. Darüber hinaus werden Massnahmen ergriffen, die Unbefugten den Zugang zu Datenverarbeitungssystemen, die personenbezogene Daten verarbeiten und/oder nutzen, verwehren. Dies geschieht durch die Anwendung der folgenden Grundsätze:

- Kenntnisnahme erforderlich. Der Zugang wird ausschliesslich auf der Grundlage dessen gewährt, was ein Mitarbeiter zur Ausübung seiner Tätigkeit benötigt.
- Geringste Berechtigung. Das minimale Zugriffsrecht wird für jeden definierten Zugriff berücksichtigt und zugewiesen.
- Aufgabentrennung (auch bekannt als Intressenskonflikt). Die Zugangsanträge unterliegen einer "Vier-Augen-Prüfung" und Kontrolle.

Anfragen für zusätzlichen Zugang folgen einem formalen Prozess, der eine Anfrage und eine Genehmigung von einem Daten- oder Systemeigentümer, Manager oder anderen Führungskräften beinhaltet, wie es die Sicherheitsrichtlinien von Yokoy vorschreiben. Darüber hinaus wird kein permanenter Zugang zur Produktionsumgebung von Yokoy gewährt.

Trennungskontrolle

In Anbetracht der mandantenfähigen Natur der Yokoy-Angebote wurden Massnahmen zur Datentrennung vollständig umgesetzt. Dies umfasst unter anderem 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.

Integrität

Die folgenden Kontrollen gewährleisten die Integrität der personenbezogenen Daten.

Übertragungskontrolle

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. Es wird der Advanced Encryption Standard (AES-256) verwendet, und jeder Verschlüsselungsschlüssel ist selbst mit einem regelmässig rotierenden Satz von Hauptschlüsseln verschlüsselt.

Eingabekontrolle

Yokoy prüft alle eingegebenen Daten auf Richtigkeit, Vollständigkeit und Konsistenz. Es gibt Kontrollen, die sicherstellen, dass 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 Frage, wer die Änderungen wann vorgenommen hat. Die Cloud-Auditprotokolle werden in einem hochgradig geschützten Speicher abgelegt, was zu einem sicheren, unveränderlichen und äusserst dauerhaften Audit-Trail führt.

Verfügbarkeit und Ausfallsicherheit

Yokoy garantiert, dass personenbezogene Daten gegen das Risiko der versehentlichen Zerstörung oder des Verlusts geschützt sind. Yokoy verwendet eine serverlose Architektur, bei der alle Backend-Dienste nach Bedarf skaliert werden. Die Datenbank wird automatisch in einem separaten (verschlüsselten) Cloud-Speicherbehälter mit einer Aufbewahrungsfrist von 1 Monat und einer täglichen Sicherungsfrequenz gesichert. Die Datensicherung ist gegen unbefugten Zugriff geschützt. Die Datenwiederherstellungsroutinen werden regelmässig getestet.

Der laufende Betrieb wird durch eine kontinuierliche Kapazitätsplanung und -überwachung sichergestellt.

Verfügbarkeitskontrolle

Yokoy verfügt über einen Business Continuity Plan (BCP), der der ISO-Norm 27001 entspricht und die bestehenden Sicherheitsvorkehrungen und Massnahmen für den Fall eines längeren Ausfalls von Diensten aufgrund von Faktoren, die sich der Kontrolle entziehen (z. B. Naturkatastrophen, von Menschen verursachte Ereignisse), beschreibt, mit dem Ziel, die Dienste in einem möglichst kurzen Zeitraum wiederherzustellen. Der Plan wird halbjährlich überprüft und jährlich erprobt.

Yokoy arbeitet mit 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.

Regelmässige Überprüfung, Bewertung und Evaluierung

Yokoy hat einen Rahmen für den Datenschutz geschaffen und entsprechende Prozesse eingerichtet, um eine angemessene Überwachung, Bewertung und Evaluierung des Datenschutzes zu gewährleisten.

Datenschutz-Management

Yokoy hat einen internen Vollzeit-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 im EU- und US-Recht (CIPP/E bzw. CIPP/US) zertifiziert ist.

Eine öffentlich zugängliche Datenschutzrichtlinie und eine Cookie-Richtlinie informieren über den Ansatz von Yokoy in Bezug auf den Datenschutz, während die Kunden ein Addendum zur Datenverarbeitung als Anhang zu ihrer SaaS-Vereinbarung unterzeichnen. Auftragsverarbeitungsverträge gibt es auch für unsere Auftragsbearbeiter, wobei wir bestrebt sind, Auftragsbearbeiter einzusetzen, die Daten ausschliesslich in der EU speichern, soweit dies möglich ist.

Es wurde eine Folgenabschätzung für den Datentransfer durchgeführt, und die Entwicklungen im Bereich der Datenübermittlung werden aufmerksam verfolgt. Durch die regelmässige Teilnahme an On-

und Offline-Veranstaltungen und das Abonnement einschlägiger Datenschutz-Newsletter wird sichergestellt, dass Yokoy den Überblick über dieses äusserst dynamische Rechtsgebiet behält.

Management der Reaktion auf Zwischenfälle

Die betriebliche Verfügbarkeit der Software wird regelmässig überprüft, und es gibt einen Geschäftskontinuitätsplan. Es werden entsprechende Meldekanäle definiert und Zuständigkeiten festgelegt, um bei Bedarf effektiv und zeitnah auf Vorfälle reagieren zu können. Zu diesem Zweck wurden die folgenden Massnahmen ergriffen:

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

Die gewonnenen Erfahrungen und Erkenntnisse fliessen in die weitere Gestaltung und Verbesserung der Prozesse ein.

Auftragskontrolle

Es wurden Massnahmen ergriffen, um sicherzustellen, dass personenbezogene Daten, die im Auftrag eines Kunden verarbeitet werden, nur in Übereinstimmung mit den Anweisungen des Kunden verarbeitet werden können. Dies wird in einem Auftragsverarbeitungsvertrag ausführlich beschrieben und von Yokoy und dem Kunden als Teil der Software-as-a-Service-Vereinbarung gemeinsam unterzeichnet.

Datenschutzfreundliche Voreinstellungen

Datenschutz durch Design

Personenbezogene Daten werden nur erhoben, wenn dies unbedingt erforderlich ist (angegebener Zweck). Dazu gehören der Name des Mitarbeiters, seine E-Mail-Adresse, die Hauptkostenstelle, die Rechtsperson (erforderlich für die Zuordnung von Ausgaben) sowie Spesenabrechnungen und -belege.

Die Unternehmensdaten sind streng getrennt, der Zugriff der Nutzer erfolgt über einen eigenen Mandanten.Standardeinstellungen stellen sicher, dass personenbezogene Daten nur in Übereinstimmung mit dem jeweiligen Verarbeitungszweck verarbeitet werden. Dank des kontinuierlichen Sensibilisierungs- und Schulungsprozesses im Rahmen des Datenschutzmanagements sind die Mitarbeiter vorsichtig im Umgang mit personenbezogenen Daten und betrachten den Datenschutzgrundsatz der Datenminimierung als Teil der Entwicklung von technischen und geschäftlichen Prozessen.