Auftragsdatenverarbeitungsvertrag

Anhang 1 zu SaaS-Vertrag vialo
(Fassung vom 24.05.2024)

Die **Kundin** als Auftraggeberin (im Sinne des DSG bzw. nach DSGVO «Verantwortlicher») wird nachfolgend als «Auftraggeberin» oder «Kundin» bezeichnet.

Xmatik als Auftragnehmerin (im Sinne des DSG «Auftragsbearbeiter», bzw. nach DSGVO «Auftragsverarbeiter») wird nachfolgend als «Xmatik» oder «Auftragnehmerin» bezeichnet.

1 Vertragsgegenstand

Dieser Auftragsdatenverarbeitungsvertrag konkretisiert die Verpflichtungen der Parteien zum Datenschutz, die sich aus dem «SaaS-Vertrag vialo» (nachfolgend «Hauptvertrag» genannt) zwischen den Parteien ergeben. Massgebend sind insbesondere die folgenden gesetzlichen Bestimmungen: a) Für Kunden in Ländern der Europäischen Union: die Datenschutz-Grundverordnung (DSGVO); b) für Kunden in der Schweiz: das schweizerische Datenschutzgesetz (DSG), die Verordnung zum Datenschutzgesetz (DSV) sowie gegebenenfalls zusätzlich ebenfalls die DSGVO (z.B. bei Verarbeitung von personenbezogenen Daten von in der EU wohnhaften Personen).

Dieser Vertrag findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen durch Xmatik personenbezogene Daten («Daten») der Auftraggeberin verarbeitet werden.

2 Vertragsbeginn und -dauer

Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den Bestimmungen dieser Regelung nicht darüberhinausgehende Verpflichtungen ergeben.

Die Verarbeitung erfolgt, solange die Auftraggeberin «vialo» nutzt und ihre Daten in der Software «vialo» gespeichert sind. Es gelten die Bestimmungen des Hauptvertrags. Der Vertrag kann mit einer Frist von 3 Monaten von beiden Parteien gekündigt werden. Er endet ebenfalls automatisch mit Beendigung des Hauptvertrags.

3 Umfang der Datenverarbeitung

3.1 Auftragserteilung

Die Auftraggeberin bestätigt, dass sie selbst berechtigt ist, diese Daten so zu bearbeiten, wie sie es in Auftrag gibt. Sie ist zudem berechtigt, Dritte mit dieser Bearbeitung zu beauftragen. Der Datenübertragung und dem Bearbeitungsauftrag stehen seitens der Auftraggeberin keine gesetzlichen oder vertraglichen Geheimhaltungspflichten entgegen.

Die Auftragnehmerin darf die personenbezogenen Daten ausschliesslich gemäss ihrem Vertrag mit der Auftraggeberin bearbeiten, gemäss den Weisungen der Auftraggeberin und den geltenden rechtlichen Grundlagen.

3.2 Verwendung der Daten

Der Gegenstand der Datenbearbeitung, ihre Art, ihr Zweck, die Art der personenbezogenen Daten und die Kategorien betroffener Personen ergeben sich in erster Linie aus dem Hauptvertrag. Xmatik verarbeitet personenbezogene Daten der Auftraggeberin als Auftragsdatenverarbeiterin aber insbesondere in den folgenden Fällen:

- Bei der Speicherung von Daten der Kundin durch Nutzung der Software «vialo» über das Internet. In diesem Fall werden personenbezogene Daten bearbeitet, die durch die Auftraggeberin in der Software «vialo» gespeichert werden (z.B. Personendaten über Mitarbeitende der Auftraggeberin).
- Bei der Analyse und zur Behebung von Softwarefehlern gemäss Hauptvertrag. In diesem Fall ist es möglich, dass die Auftragnehmerin Zugriff auf Daten der Auftraggeberin erhält. Davon können auch Personendaten betroffen sein.
- Bei der Migration von Daten aus externen Systemen (z.B. «Xtacho») nach «vialo» gemäss Auftrag der Kundin. In diesem Fall werden personenbezogene Daten nur so weit verarbeitet, wie die Auftraggeberin diese zur Migration nach «vialo» vorsieht und an Xmatik anliefert (z.B. Personendaten über Mitarbeitende der Auftraggeberin)

Abhängig von den durch die Auftraggeberin übermittelten Daten können folgende Kategorien von Personen von einer Datenverarbeitung betroffen sein:

- Mitarbeitende der Auftraggeberin
- Lieferanten und Dienstleister der Auftraggeberin (z.B. Fremdfahrer)
- Kunden und Interessenten der Auftraggeberin
- Ansprechpartner der Auftraggeberin

Je nach Nutzung der Software durch die Auftraggeberin können insbesondere folgende Personendaten Gegenstand der Datenverarbeitung sein:

- Personenstammdaten (z.B. Name, Geburtsdatum, Führerausweisangaben) einschliesslich Kontakt- oder Kommunikationsdaten (z.B. Telefon, E-Mail, Adresse)
- Aufzeichnungen über Arbeits- und Ruhezeiten
- Fahrzeugstandort- und Fahrzeugbewegungsdaten
- Auftrags- und Vertragsdaten einschliesslich deren Historie
- Vertragsabrechnungs- und Zahlungs- sowie Akquisitionsdaten

Die Auftraggeberin stellt sicher, dass keine besonders schützenswerten Daten gemäss Art. 5 DSG (Art. 9 DSGVO) gespeichert werden. Dies umfasst die folgenden Datenkategorien:

- rassische und ethnische Herkunft
- politische Meinungen
- religiöse oder weltanschauliche Überzeugungen
- Gewerkschaftszugehörigkeit
- genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person
- Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung

Bei der Speicherung solcher Daten ist die Auftragnehmerin unverzüglich zu informieren. Die Auftragnehmerin behält sich vor, in diesem Fall den Vertrag unverzüglich einseitig zu beenden.

3.3 Ort der Datenverarbeitung

Die Verarbeitung der Daten findet grundsätzlich in der Schweiz statt. Ein angemessenes Datenschutzniveau nach DSGVO wurde von der EU-Kommission in einer förmlichen Entscheidung für die Schweiz festgestellt (2000/518/EC).

Die Auftraggeberin nimmt zur Kenntnis, dass gewisse von der Auftragnehmerin eingesetzte Dienste auch auf physischen Servern eines Dritten und/oder in Public Cloud-Diensten (z.B. Microsoft Azure) betrieben werden können. In diesem Fall werden die entsprechenden Dienste nach den Rechten und Pflichten von Unterauftragsverarbeiten gemäss Ziffer 4.3 geführt und durch die Auftragnehmerin bekannt gegeben. Die Auftragnehmerin stellt dabei sicher, dass diese einen angemessenen Schutz der Daten gemäss den gesetzlichen Bestimmungen gewährleistet und nutzt möglichst Dienste, die auf Servern in der Schweiz oder in einem Mitgliedsstaat des Europäischen Wirtschaftraums (EWR) betrieben werden. Werden Datenverarbeitungstätigkeiten ausnahmsweise auch ausserhalb des EWR durchgeführt, stellt die Auftragnehmerin

vorgängig ein angemessenes Datenschutzniveau mittels geeigneter Garantien gemäss gesetzlichen Bestimmungen sicher.

4 Rechte und Pflichten

4.1 Datensicherheit (technische und organisatorische Massnahmen)

Die Auftragnehmerin hat für eine ausreichende Sicherheit der Daten zu sorgen. Insbesondere hat Xmatik dafür zu sorgen, dass diese Daten nicht unberechtigten Dritten zugänglich gemacht oder bekannt werden.

Die Auftragnehmerin stellt durch geeignete technische und organisatorische Massnahmen sicher, dass die Daten gemäss den gesetzlichen Bestimmungen bearbeitet und alle Massnahmen ergriffen werden, damit die Datensicherheit gewährleistet ist. Es handelt sich um Massnahmen zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Die Auftragnehmerin sorgt insbesondere auch dafür, dass bei der Erfassung, Bearbeitung und Übermittlung von Personendaten die Datensicherheit angemessen gewährleistet ist.

Die zum Zeitpunkt des Vertragsabschlusses eingesetzten technischen und organisatorischen Massnahmen («TOMs») sind in Anlage A dieses Auftragsdatenverarbeitungsvertrags aufgeführt und Bestandteil dieses Vertrags. Dabei wurden der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Datenschutzrechte von Personen berücksichtigt. Die technischen und organisatorischen Massnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es der Auftragnehmerin gestattet, alternative adäquate Massnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Massnahmen nicht unterschritten werden. Wesentliche Änderungen werden dokumentiert und die jeweils aktuelle Fassung ist auf der Webseite www.vialo.ch abrufbar.

4.2 Geheimhaltung

Xmatik verpflichtet sich, die von der Auftraggeberin zur Bearbeitung anvertrauten Daten geheim zu halten.

Die Auftragnehmerin stellt sicher, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Mitarbeitenden und weiteren Hilfspersonen ebenfalls zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

Die Vertraulichkeitspflicht besteht auch nach Beendigung des Hauptvertrags weiter.

4.3 Einsatz von Unterauftragsverarbeitern

Die Auftraggeberin ist ausdrücklich damit einverstanden, dass die Auftragnehmerin für bestimmte Datenverarbeitungen aus dem Hauptvertrag, beispielsweise für das Daten-Hosting, Subunternehmen beauftragen darf. Die Beauftragung solcher Unterauftragsverarbeiter durch die Auftragnehmerin ist zulässig, soweit diese im Umfang des Unterauftrags ihrerseits die Anforderungen des vorliegenden Vertrags erfüllen. Die Auftragnehmerin trifft mit den Unterauftragsverarbeitern im erforderlichen Umfang Vereinbarungen, um angemessene Datenschutz- und Informationssicherheitsmassnahmen zu gewährleisten.

Eine Liste der aktuell eingesetzten Subunternehmen im Sinne von Unterauftragsverarbeitern ist auf der Webseite www.vialo.ch abrufbar. Vor Hinzuziehung weiterer Subunternehmen aktualisiert Xmatik mindestens 14 Tage vorher die Liste auf der Webseite. Die Auftraggeberin wird die Liste regelmässig einsehen, um über Änderungen informiert zu sein und kann der Änderung innert 14 Tagen seit Kenntnisnahme aus wichtigem datenschutzrechtlichem Grund widersprechen. Sofern eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich ist, kann die Auftragnehmerin den Vertrag aus wichtigem Grund fristlos kündigen.

4.4 Einsichts- und Kontrollrechte

Xmatik weist der Auftraggeberin auf Aufforderung die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach. Dadurch entstehende Aufwände kann die Auftragnehmerin der Auftraggeberin in Rechnung stellen. Sollte im Einzelfall eine Prüfung durch die Auftraggeberin oder von ihr beauftragte Dritte benötigt werden, ist diese zu den üblichen Geschäftszeiten durchzuführen unter Berücksichtigung einer angemessenen Vorlaufzeit.

4.5 Anfragen betroffener Personen und Aufsichtsbehörden

Die Auftraggeberin bleibt zuständig für Auskunftsbegehren, Behördenkontakte und andere Stellungnahmen betreffend ihrer Daten und deren Bearbeitung.

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an Xmatik, wird Xmatik die betroffene Person an die Auftraggeberin verweisen. Xmatik kann die Auftraggeberin gegen aufwandsbasierte Entschädigung bei der Beantwortung dieser Anfragen unterstützen.

Xmatik erteilt den für die Auftraggeberin zuständigen Aufsichtsbehörden auf deren erstes Verlangen hin alle Auskünfte und übergibt ihnen sämtliche Unterlagen, die diese zur Erfüllung ihrer Aufgaben benötigen. Entsprechende Leistungen kann sie der Auftraggeberin nach Aufwand verrechnen.

4.6 Löschung und Rückgabe personenbezogener Daten

Die Herausgabe der Daten und die entsprechende Vergütung ist im Hauptvertrag geregelt.

4.7 Verletzungen von Datenschutz- und Geheimhaltungspflichten

Xmatik unterrichtet die Auftraggeberin unverzüglich, wenn ihr Verletzungen des Schutzes personenbezogener Daten der Kundin bekannt werden. Die Auftragnehmerin trifft die erforderlichen Massnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit der Auftraggeberin ab.

5 Weitere Bestimmungen

Im Übrigen gelten die Bestimmungen des Hauptvertrags. Bei etwaigen Widersprüchen zwischen dem Auftragsdatenverarbeitungsvertrag und dem Hauptvertrag gehen die Bestimmungen des Hauptvertrags vor. Sollten einzelne Teile des Auftragsdatenverarbeitungsvertrags unwirksam sein, so berührt dies die Wirksamkeit des Hauptvertrags und der übrigen Bestimmungen des Auftragsdatenverarbeitungsvertrages nicht.

Änderungen und Ergänzungen dieser Zusatzvereinbarung bedürfen zu ihrer Wirksamkeit der Schriftform und Unterzeichnung durch die Parteien.

Anlage A: Technische und organisatorische Massnahmen

Vertraulichkeit

Zutrittskontrolle / Benutzerkontrolle

Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen:

- Festlegung von Sicherheitsbereichen
- Wirksamer Zutrittsschutz durch Schlüssel mit Chipkarten
- Festlegung zutrittsberechtigter Personen und Schlüsselregelung (Schlüsselausgabe etc.)
- Sorgfältige Auswahl von Reinigungspersonal und Hausdienst
- Begleitung von Besuchern und Fremdpersonal
- Jeder kennt jeden (KMU)
- Integritätsprüfung des Personals

Zusätzliche Massnahmen im Daten-Hosting durch EGELI Informatik AG:

- Zutrittsberechtigungsstruktur ist auf das Notwendigste beschränkt
- Videoüberwachung
- Biometrische Zugangskontrolle
- Vereinzelungsanlage

Zugangskontrolle

Schutz vor unbefugter Systembenutzung:

- Authentifikation mit Benutzername + Passwort
- Zwei-Faktor-Authentifizierung für externe Zugriffe
- Verschlüsselung von mobilen Datenträgern und Laptops
- Zuordnung von Benutzerrechten über Benutzerprofile
- Einsatz von Anti-Viren-Software und Intrusion Detection Systemen
- Einsatz von Firewalls und Proxy-Servern
- Einsatz von VPN-Technologie

Zusätzliche Massnahmen im Daten-Hosting durch EGELI Informatik AG:

- Zugriff auf Backend-Systeme ausschliesslich von persönlichen, in separaten Netzwerken geführten Arbeitsplätzen (VDI)

Zugriffskontrolle

Schutz vor unbefugtem Lesen, Kopieren, Verändern oder Entfernen von Daten:

- Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte (Berechtigungsprofile mit Minimalrechten, «Least Privilege Prinzip»)
- Prozesse für Berechtigungsvergabe
- Protokollierung von Zugriffen
- Passwortrichtlinie inkl. Passwortlänge und -komplexität
- Periodische Überprüfung der vergebenen Berechtigungen, insbesondere von administrativen Benutzerkonten
- Sichere Aufbewahrung von Datenträgern
- Ordnungsgemässe Vernichtung von Datenträgern

Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden:

- Trennung von Produktiv- und Testumgebungen
- Softwarebasierte Mandantentrennung
- Steuerung über Berechtigungskonzept
- Festlegung von Datenbankrechten

Integrität

Weitergabekontrolle / Datenträgerkontrolle

Schutz vor unbefugtem Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport:

- Bereitstellung über verschlüsselte Verbindungen wie SFTP und HTTPS und Vermeidung unsicherer und veralteter Protokolle wie z.B. TLS 1.0, 1.1
- Einsatz von VPN
- Protokollierung der Zugriffe und Abrufe
- Sichere Aktenvernichtung

Eingabekontrolle / Speicherkontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

- Validierungsvorgänge in Applikationen
- Protokollierung der Eingabe und Änderung personenbezogener Daten
- Nachvollziehbarkeit durch persönliche Benutzerkonten
- Änderungen an Datenbanken ausschliesslich im 4-Augen-Prinzip
- Regelmässige Validierung der Firewall Rules

Verfügbarkeit

Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust (Massnahmen im Daten-Hosting durch EGELI Informatik AG):

- Unabhängige Strompfade
- Überbrückung durch USV- und Netzersatzanlagen
- Photovoltaik am gesamten Gebäude des Rechenzentrums
- Adiabatische Kühlung ohne mechanische Kältemaschinen
- Redundant ausgelegte Kernsysteme
- Automatisierte Restoretests
- Regelmässige Disaster Recovery-Übungen
- Business Continutity Plan
- Umfassendes Backup Konzept (online/offline, onsite/offsite) mit Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- SLA mit Lieferanten (Hardware, Netzwerk und Security, Cybervorfälle)