Vereinbarung Auftragsverarbeitung (AVV) oqio analytiqs

Diese Vereinbarung Auftragsverarbeitung (AVV) regelt die Datenverarbeitung im Auftrag des Auftraggebers durch die oqio GmbH (nachfolgend „oqio“) als Auftragnehmer. Sie ist Bestandteil des Vertrages zwischen oqio und dem Auftraggeber.

1. Vertragsgegenstand, Inhalt des Auftrags

1.1 oqio erbringt die Bereitstellung von oqio analytiqs (nachfolgend „Software“) auf Grundlage des Vertrages zwischen dem Auftraggeber und oqio (nachfolgend „Hauptvertrag“).

1.2 Zur Konkretisierung der datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung Auftragsverarbeitung. Gegenstand und Dauer der Leistungserbringung durch oqio richten sich nach dem Hauptvertrag. Die Regelungen der vorliegenden Vereinbarung Auftragsverarbeitung gehen im Zweifel den Regelungen des Hauptvertrags vor.

2. Umfang, Zweck und Durchführung der Datenverarbeitung; Art der Daten und Kreis der Betroffenen; Weisungsgebundenheit

2.1 Umfang und Zweck der Datenverarbeitung durch oqio ergeben sich aus dem Hauptvertrag und der dazugehörigen Leistungsbeschreibung.

2.2 oqio hat im Rahmen der Leistungserbringung potentiell Zugriff auf die in der Software gespeicherten Daten. Dabei handelt es sich um folgende Datenkategorien und potentiell Betroffene:

- Mitarbeiter des Auftraggebers:
  - Nutzeraccounts (einschließlich Name, Benutzerkennung, E-Mail-Adresse, Passwort)
- Endkunden des Auftraggebers sowie weitere Personen, die vom Auftraggeber oder dessen Endkunden in der Software erfasst werden (z.B. Ansprechpartner beim Versicherer, Verwalter, Handwerker/Dienstleister, Schadensverursacher usw.):
  - Kontaktdaten (Namen, Telefonnummer, E-Mail-Adressen)
  - Nutzeraccounts (einschließlich Name, Benutzerkennung, E-Mail-Adresse, Passwort)
  - Schadensdaten (z.B. Schadensdokumentation, Informationen über Schadensbehebung, Angebote)
  - Kommunikation (z.B. Mitteilungen an andere Beteiligte, Anmerkungen zu Dokumenten und Vorgängen)

Zudem fallen beim Betrieb der Software allgemeine Webserver-Logdaten an.

2.3 oqio darf personenbezogene Daten des Auftraggebers ausschließlich zu Zwecken der Erfüllung des Hauptvertrags im Auftrag des Auftraggebers oder aufgrund von Einzelweisungen des Auftraggebers verarbeiten. Sofern oqio Daten aufgrund einer rechtlichen Verpflichtung im Sinne des Art. 28 Abs. 3 lit. a DSGVO verarbeitet, teilt oqio dies dem Auftraggeber vor der Verarbeitung mit, soweit dies nicht rechtlich ausgeschlossen ist. Der Auftraggeber gestattet oqio zudem die Einbindung eines Web-Analysetools (z.B. Google Analytics) in das SaaS-System zur Erhebung anonymisierter Nutzungsstatistiken zu eigenen Zwecken. Die Erstellung der Nutzungsstatistiken soll – soweit erforderlich – nur mit Einwilligung („Opt In“) der Endnutzer erfolgen. Darüber hinaus darf oqio aus den in der Software vorhandenen Datenbeständen anonyme, aggregierte Statistiken erstellen (z.B. Statistiken über die Anzahl der angelegten Nutzer oder Dokumente).

2.4 oqio hat Einzelweisungen des Auftraggebers über die Erhebung, Verarbeitung oder Nutzung von Daten zu beachten und umzusetzen. Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen in Textform berechtigt. Dies umfasst auch Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten. Ist oqio der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, wird oqio den Auftraggeber darauf hinweisen. Die angemessenen Kosten der Durchführung von Weisungen, die über die vertraglichen Leistungen des Hauptvertrags hinausgehen, werden vom Auftraggeber nach Maßgabe der jeweils geltenden Stundensätze von oqio erstattet.

3. Unterauftragsverhältnisse

3.1 oqio ist zur Einschaltung von weiteren Auftragsverarbeitern als Unterauftragsverarbeiter berechtigt. Derzeit setzt oqio die folgenden Unterauftragsverarbeiter ein:

- Amazon Web Services EMEA SARL, Luxemburg (Hosting der Software)
- Strato AG, Deutschland (Backup)
- Twilio Inc., USA (Transaktions-E-Mails)

Vertragliche Vereinbarungen mit Unterauftragsverarbeitern werden durch oqio so gestaltet, dass sie den Bestimmungen der DSGVO entsprechen.

3.2 oqio informiert den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Unterauftragsverarbeiter, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch

zu erheben. Sollte der Auftraggeber begründete Einwände gegen den Einsatz eines solchen neuen Unterauftragsverarbeiters haben, ist der Auftraggeber berechtigt, gegenüber oqio innerhalb von 14 Tagen nach Erhalt der Änderungsmitteilung Einspruch gegen den Einsatz des Unterauftragsverarbeiters zu erheben. Sofern oqio daraufhin trotz berechtigten Einspruchs gegenüber dem Auftraggeber erklärt, dass nicht aufgrund des Einspruchs auf den Einsatz des Subunternehmers verzichtet wird, ist der Auftraggeber berechtigt, den Hauptvertrag mit einer Frist von vier Wochen schriftlich zu kündigen.

3.3 Als Unterauftragsverarbeitungsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören insbesondere Nebenleistungen, die oqio z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern in Anspruch nimmt. oqio ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

4. Datengeheimnis und Vertraulichkeit

oqio stellt sicher, dass die zur Verarbeitung der personenbezogenen Daten eingesetzten Mitarbeiter zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung des Arbeitsverhältnisses zwischen dem Mitarbeiter und oqio bestehen bleiben.

5. Schutzmaßnahmen und Kontrolle

5.1 oqio trifft die gemäß Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen, insbesondere wie in **Anlage 1** näher beschrieben. oqio kann die technischen und organisatorischen Maßnahmen ändern und anpassen, insbesondere an Fortentwicklungen des Standes der Technik, sofern dadurch das anfängliche Sicherheitsniveau nicht unterschritten wird.

5.2 oqio stellt dem Auftraggeber auf Anfrage alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten gemäß Art. 28 DSGVO zur Verfügung, z.B. durch Vorlage geeigneter Dokumentation. oqio ermöglicht zudem die Überprüfung durch den Auftraggeber oder einen anderen von diesem beauftragten Prüfer. Zu diesem Zweck gestattet oqio dem Prüfer, sich nach Anmeldung zu Prüfzwecken in den Betriebsräumen von oqio zu den üblichen Geschäftszeiten ohne erhebliche Störung des Betriebsablaufes von der Einhaltung der für die Auftragsverarbeitung einschlägigen Pflichten zu überzeugen. Die angemessenen Kosten der Mitwirkung bei einer solchen Prüfung auf Seiten von oqio werden vom Auftraggeber nach Maßgabe der Stundensätze von oqio erstattet.

5.3 Der Auftraggeber verpflichtet sich, alle im Rahmen der vorgenannten Kontrollen und Auskünfte bekannt gewordenen oder von oqio bekannt gegebenen Informationen, Unterlagen, Daten und Erkenntnisse streng vertraulich zu behandeln, ausschließlich für die datenschutzrechtliche Kontrolle zu verwenden und nicht anderweitig zu nutzen. Vom Auftraggeber eingeschaltete Mitarbeiter oder externe Dritte sind, sofern sie nicht von Berufs wegen zur Verschwiegenheit verpflichtet sind, einer gleichwertigen Verschwiegenheitspflicht wie der hier festgelegten zu unterwerfen.

6. Informations- und Unterstützungspflichten

6.1 Wenn oqio eine Verletzung des Schutzes personenbezogener Daten des Auftraggebers bekannt geworden ist, meldet oqio diese unverzüglich dem Auftraggeber. oqio wird im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene ergreifen. oqio unterstützt den Auftraggeber bei der Erfüllung der Melde- und Benachrichtigungspflichten gemäß Art. 33 und 34 DSGVO.

6.2 oqio unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Erstellung von Datenschutzfolgenabschätzungen gemäß Art. 35, 36 DSGVO. Die angemessenen Kosten der Unterstützung durch oqio werden vom Auftraggeber nach Maßgabe der Stundensätze von oqio erstattet.

6.3 Sollten die Daten bei oqio durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat oqio den Auftraggeber unverzüglich darüber zu informieren. oqio wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als Verantwortlichem im Sinne der DSGVO liegen.

7. Löschung von Daten

7.1 Die Löschung der im Rahmen des Auftragsverhältnisses erhobenen, verarbeiteten und genutzten Daten erfolgt jederzeit auf Weisung des Auftraggebers und bei Beendigung des Hauptvertrages entsprechend der Regelung im Hauptvertrag (Ziffer 14.3), sofern jeweils keine für oqio relevanten gesetzlichen Aufbewahrungsfristen einschlägig sind. Für die Wahrung der den Auftraggeber betreffenden gesetzlichen Aufbewahrungsfristen ist der Auftraggeber verantwortlich.

7.2 Sofern im Zuge der Datenverarbeitung Datenträger vom Auftraggeber überlassen worden sind, wird oqio diese spätestens mit Beendigung des Hauptvertrages zurückgeben.

8. Rechte der betroffenen Personen

8.1 Soweit ein Betroffener sich unmittelbar an oqio zwecks Wahrnehmung von Betroffenenrechten (z.B. bezüglich der Berichtigung, Sperrung bzw. Einschränkung der Verarbeitung oder Löschung von Daten) wenden sollte, wird oqio dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

8.2 oqio unterstützt den Auftraggeber auf Anforderung bei der Wahrung dieser Rechte, z.B. im Hinblick auf die Informationspflichten (Benachrichtigung, Auskunftserteilung), Berichtigung, Sperrung bzw. Einschränkung der Verarbeitung und Löschung personenbezogener Daten. Die angemessenen Kosten der Unterstützung durch oqio werden vom Auftraggeber nach Maßgabe der Stundensätze der oqio erstattet.

9. Laufzeit und Schlussbestimmungen

9.1 Die vorliegende Vereinbarung Auftragsverarbeitung endet mit der Beendigung des Hauptvertrags. Sie bleibt auch über die Beendigung des Hauptvertrags hinaus solange in Kraft, wie oqio über personenbezogene Daten des Auftraggebers verfügt.

9.2 Die zwischen den Parteien im Hauptvertrag vereinbarte Haftungsregelung gilt auch für die Haftung zwischen den Parteien im Zusammenhang mit dieser Vereinbarung Auftragsverarbeitung.

9.3 Änderungen und Ergänzungen dieser Vereinbarung Auftragsverarbeitung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

9.4 Es gilt ausschließlich deutsches Recht unter Ausschluss solcher Rechtsnormen, die auf andere Rechtsordnungen verweisen. Das einheitliche UN-Kaufrecht (UNCITRAL) findet keine Anwendung.

Anlage 1 zur Vereinbarung Auftragsverarbeitung
Technische und organisatorische Maßnahmen (TOMs)

Vorbemerkung

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die oqio für die Software mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen. Diese Maßnahmen werden ergänzt durch technische und organisatorische Maßnahmen des von oqio eingesetzten Unterauftragsverarbeiters für Server- und Rechenzentrums-Dienstleistungen.

Die TOMs werden wie folgt gruppiert:
- System (Server, Datenbanken usw.)
- Anwendungssoftware
- Lokale IT-Infrastruktur von oqio (Desktop, Laptop usw.)

Die unterschiedlichen technischen und organisatorischen Maßnahmen pro Zugriffsart sind separat aufgelistet oder allgemein definiert.

Die Backend-Systeme (Server, Datenbanken usw.) werden von einem Unterauftragsverarbeiter betrieben. Der Unterauftragsverarbeiter setzt insoweit angemessene Sicherheitsmaßnahmen um und ist nach ISO27001 zertifiziert.

1. Verfahren und Anforderungen zur Gewährleistung der Verfügbarkeit der personen-bezogenen Daten

Gewährleisten, dass Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Um dies zu gewährleisten müssen mindestens folgende Maßnahmen durch oqio ergriffen werden:

Software:
- Backup-Verfahren / -konzept
- Funktionstrennung (Produktion- / Testsysteme)

Arbeitsplatz:
- Benutzer - Backup-Verfahren / -konzept
- Virenschutz
- Brandschutzmaßnahmen (Feuerlöscher, Brandmelder usw.)

2. Verfahren und Anforderungen zur Gewährleistung der Vertraulichkeit der personen-bezogenen Daten

Verhindern, dass Unbefugte Zutritt zu den Verarbeitungsanlagen haben. Um dies zu gewährleisten müssen mindestens folgende Maßnahmen durch oqio ergriffen werden:

Arbeitsplatz:
- Schlüssel / Protokollierung der Schlüsselvergabe
- Mechanische Türsicherung
- Begleitung durch einen internen Mitarbeiter

Verhindern, dass Unbefugte Verarbeitungsanlagen nutzen können. Um dies zu gewährleisten müssen mindestens folgende Maßnahmen durch oqio ergriffen werden:

Software:
- Verschlüsselte Verbindung (HTTPS)
- Kennwortverfahren (u.a. Mindestlänge, Zahl, Groß- und Kleinschreibung, usw.)
- Verschlüsselte Speicherung von Passwörtern (z.B. PBKBF2)
- Aktualität der verwendeten Software (Sicherheitspatches)

Arbeitsplatz:
- Virenschutz
- Kennwortverfahren (u.a. Mindestlänge, Zahl, Groß- und Kleinschreibung, usw.)
- Automatische Sperrung (z.B. Kennwort oder Pausenschaltung)
- Einrichtung eines Benutzerstammsatzes pro User
- Aktualität der verwendeten Software (max. 1 Jahr alt, regelmäßiges Einspielen von Sicherheitspatches)
- Verschlüsselung von Arbeitsplatzfestplatten
- Sichtschutz (Fensterplätze, unterwegs)

3. Verfahren und Anforderungen zur Gewährleistung der Integrität der personenbezogenen Daten

Gewährleisten, dass nur Berechtigte auf Daten zugreifen können und diese nicht unbefugt gelesen, verändert, kopiert oder entfernt werden können. Um dies zu gewährleisten müssen mindestens folgende Maßnahmen durch oqio ergriffen werden:

Software:
- Datenschutzkonforme Löschung der Daten nach Vertragsbeendigung oder auf Verlangen des Auftraggebers
- Berechtigungskonzept mit differenzierten Berechtigungen (User, Profile und Rollen)
- Aktualität der verwendeten Software (Sicherheitspatches)

Arbeitsplatz:
- Berechtigungskonzept mit differenzierten Berechtigungen (User, Profile und Rollen)
- Verschlüsselung von Arbeitsplatzfestplatten

Gewährleisten, dass Daten bei der elektronischen Übertragung/Transport nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Um dies zu gewährleisten müssen mindestens folgende Maßnahmen durch oqio ergriffen werden:
- Die Mitarbeiter von oqio sind zur Wahrung des Datengeheimnisses gemäß DSGVO und zur Wahrung von Geschäftsgeheimnissen vertraglich verpflichtet

Sicherung bei der elektronischen Übertragung:
- Verschlüsselung (bspw. Mittels VPN)
- Authentisierung der Gegenstelle (Zertifikat)

Gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden (Speicherung, Veränderung, Löschung, Übermittlung). Um dies zu gewährleisten müssen mindestens folgende Maßnahmen zur Trennungskontrolle durch oqio ergriffen werden:

Software:
- Dedizierte (virtuelle) Server
- Funktionstrennung (Produktion- / Testsysteme)

4. Gewährleistung der Belastbarkeit bei Verfahren zur Verarbeitung der personenbezogenen Daten

Gewährleisten, dass es nicht zur Überlastung des Verfahrens zur Verarbeitung von personenbezogenen Daten kommt. Um dies zu gewährleisten müssen mindestens folgende Maßnahmen durch oqio ergriffen werden:
- Verwendung von ausreichend dimensionierter Hardware & Software

5. Verfahren und Anforderungen zur Gewährleistung Zugang zu personenbezogenen Daten bei einem physischen oder technischen Zwischenfall, rasch wiederherzustellen

Gewährleisten, dass Daten bei einem physischen oder technischen Zwischenfall, rasch wiederhergestellt werden können. Um dies zu gewährleisten müssen mindestens folgende Maßnahmen durch oqio ergriffen werden:

Software:
- Backup- und Wiederherstellungsverfahren

Arbeitsplatz:
- Benutzer - Backup-Verfahren / -konzept
- Reserve Hardware

6. Verfahren und Anforderungen zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit von technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Gewährleisten, dass oqio den regelmäßigen Nachweis der Erfüllung seiner Pflichten, insbesondere der vollständigen Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen sowie ihrer Wirksamkeit führt und dokumentiert. Um dies zu gewährleisten müssen mindestens folgende Maßnahmen durch oqio ergriffen werden:
- Audit- oder Kontrollverfahren zur Bewertung und Evaluierung der Wirksamkeit der TOMs
- Ggf. entsprechende Zertifizierung oder Verhaltensregeln
- Führung eines Verzeichnisses der Verarbeitungstätigkeiten
- Bestellung eines Datenschutzbeauftragten und Mitteilung der Kontaktdaten.

7. Sonstige Verfahren und Anforderungen

Gewährleisten, dass Daten, die im Auftrag verarbeitet werden, nur entsprechend den Anweisungen des Auftraggebers verarbeitet werden können. Um dies zu gewährleisten müssen mindestens folgende Maßnahmen zur Auftragskontrolle durch oqio ergriffen werden:

- Eindeutige Vertragsgestaltung durch AV-Vertrag (Weisungsbefugnisse, Kontrollrechte usw.)
- Verpflichtung der Mitarbeiter von oqio zur Wahrung des Datengeheimnisses gemäß DSGVO und zur Wahrung von Geschäftsgeheimnissen
- Angemessene Schulungs- und Sensibilisierungsmaßnahmen
- Führung eines Verzeichnisses der Verarbeitungstätigkeiten
- Bestellung eines Datenschutzbeauftragten und Mitteilung der Kontaktdaten