Auftragsverarbeitungsvertrag (AVV)

Die arteria GmbH ("arteria") erbringt gegenüber dem Kunden SaaS-Dienstleistungen in Bezug auf der von arteria auf seinen Websites angebotenen und in den jeweiligen Beschreibungen konkretisierten Produkten.
Bei der Erbringung dieser Dienstleistungen speichert arteria personenbezogene Daten im Auftrag und für die Zwecke des Kunden ("Auftragsverarbeitung").

1. Gegenstand und Anwendungsbereich des AVV

1.1. Dieser Auftragsverarbeitungvertrag ("AVV") regelt die Pflichten, Rollen und Zuständigkeiten von arteria und dem Kunden ("Vertragsparteien") in Bezug auf die auftragsgemässe Datenverarbeitung.

2. Gültigkeit, Laufdauer, Verhältnis zum SaaS-Vertrag

2.1. arteria stellt diesen AVV in der Administrationsoberfläche zum Abschluss in Bezug auf die vertragsgemäss erbrachten Dienstleistungen bereit. Wenn der Kunde dem AVV durch Aktivierung eines Bestätigungsfelds (Click-to-Accept) zustimmt, wird der AVV für die Vertragsparteien zum verbindlichen Bestandteil ihrer vertraglichen Vereinbarungen betreffend die Erbringung der SaaS-Dienstleistungen ("SaaS-Vertrag"). Der AVV gilt für die gesamte Dauer des SaaS-Vertrags und gegebenenfalls darüber hinaus bis zur Löschung der von der Auftragsverarbeitung betroffenen personenbezogenen Daten (vgl. Ziff. 4.2) durch arteria.

2.2. Die Bestimmungen dieses AVV ergänzen die Bestimmungen des SaaS-Vertrags. Sie schränken die Rechte und Pflichten der Vertragsparteien in Bezug auf die Erbringung bzw. die Inanspruchnahme der SaaS-Dienstleistungen nicht ein. Ihren Regelungsgegenstand betreffend gehen die Bestimmungen dieses AVV indes (sofern im SaaS-Vertrag nicht ausdrücklich anders vereinbart) den Bestimmungen des SaaS-Vertrags vor.

3. Anwendungsbereich

3.1. Dieser AVV gilt (sobald ihm der Kunde zugestimmt hat) in Bezug auf Auftragsverarbeitungen im Rahmen der von arteria gemäss SaaS-Vertrag erbrachten Dienstleistungen.

3.2. Dieser AVV gilt ausdrücklich nicht in Bezug auf Verarbeitungen personenbezogener Daten, bei denen arteria die Zwecke und Mittel der Verarbeitung bestimmt und somit unter dem Schweizerischen Bundesgesetz über den Datenschutz (DSG) oder allenfalls anwendbaren anderen Datenschutzgesetzen (insbesondere der EU-DSGVO) verantwortlich ist. Solche Verarbeitungen personenbezogener Daten, die arteria als Verantwortlicher vornimmt (z.B. Verarbeitungen personenbezogener Daten zu Zwecken der Leistungsabrechnung oder der Kommunikation mit dem Kunden) nimmt arteria in Übereinstimmung mit der Datenschutzerklärung von arteria und den anwendbaren Datenschutzgesetzen vor.

4. Angaben zur Auftragsverarbeitung

4.1. Gegenstand und Zweck der Auftragsverarbeitung ist die Erbringung von SaaS-Dienstleistungen durch arteria für den Kunden. Die Auftragsverarbeitung besteht in der Speicherung, Bereitstellung, Übermittlung und Löschung von personenbezogenen SaaS-Daten gemäss den Bestimmungen des SaaS-Vertrags.

4.2. Von der Auftragsverarbeitung betroffen sind personenbezogene Daten, die der Kunde gemäss seiner Wahl auf der von arteria für die Leistungserbringung eingesetzten Infrastruktur speichert sowie Daten von Personen mit Zugriff auf diese Infrastruktur. Dabei handelt es sich insbesondere um personenbezogene Daten, die bei der Nutzung von Applikationen üblicherweise erhoben werden. Dazu gehören Protokolldaten, die bei der informatorischen Nutzung einer Applikation automatisiert erhoben werden (z.B. die IP-Adresse und das Betriebssystem des Geräts des Nutzers sowie das Datum und die Zugriffszeit des Browsers), vom Nutzer eingegebene Daten sowie vom Kunden erhobene Nutzungsdaten mit Personenbezug (nachstehend "personenbezogene SaaS-Daten").

5. Rollen und Zuständigkeitsbereiche

5.1. Der Kunde bestätigt und arteria anerkennt, dass der Kunde für die Verarbeitung der personenbezogenen SaaS-Daten nach anwendbaren Datenschutzgesetzen verantwortlich ist und bleibt. Der Kunde nimmt somit die Rolle des Verantwortlichen ein.

5.2. arteria anerkennt, dass der Kunde in der Rolle des Verantwortlichen verpflichtet ist, arteria bei Inanspruchnahme von SaaS-Dienstleistungen einige seiner Pflichten aus der EU-DSGVO (oder anderen allenfalls anwendbaren Datenschutzgesetzen) vertraglich zu überbinden.

5.3. arteria nimmt in Bezug auf die Verarbeitung betroffener personenbezogener Daten die Rolle des Auftragsverarbeiters ein. Sofern arteria für diese Auftragsverarbeitung nicht ebenfalls der EU-DSGVO (oder den anderen allenfalls anwendbaren Datenschutzgesetzen) untersteht, so nimmt arteria diese Rolle nur auf der Grundlage der vertraglichen Pflichten von arteria gemäss diesem AVV ein und wird nicht alleine deswegen unter der EU-DSGVO (oder den anderen allenfalls anwendbaren Datenschutzgesetzen) verpflichtet.

6. Pflichten von arteria

6.1. arteria verpflichtet sich, die personenbezogenen SaaS-Daten nur zur Erbringung der SaaS-Dienstleistungen gemäss Leistungsbeschrieb und vertraglichen Pflichten sowie gemäss diesem AVV zu verarbeiten.

6.2. arteria ist dazu berechtigt, personenbezogene SaaS-Daten des Kunden so zu verarbeiten, wie es die Erfüllung der Leistungspflichten aus dem SaaS-Vertrag sowie diesem AVV beinhaltet. Auf entsprechende Anfrage ist arteria bereit, weitergehende, die Auftragsverarbeitung betreffende Weisungen des Kunden umzusetzen. Voraussetzung dafür ist, dass diese für arteria im Rahmen der vertraglich vereinbarten SaaS-Dienstleistungen umsetzbar und objektiv zumutbar sind und nicht zu Mehrkosten oder geändertem Leistungsumfang führen. Vorbehalten bleibt in jedem Fall die Erfüllung gesetzlicher oder regulatorischer Pflichten, denen arteria unterliegt.

6.3. arteria sorgt für die Einhaltung der Bestimmungen dieses AVV durch die mit der Auftragsverarbeitung betrauten Mitarbeiter und anderen für arteria tätigen Personen, die Zugriff auf die personenbezogenen SaaS-Daten erhalten. arteria verpflichtet sich zudem, Personen mit Zugang zu den personenbezogenen SaaS-Daten zur Wahrung der Vertraulichkeit (auch über die Dauer ihrer Tätigkeit für arteria hinaus) zu verpflichten.

6.4. arteria verpflichtet sich, im Interesse der Vertraulichkeit, Integrität und vertragsgemässen Verfügbarkeit der personenbezogenen SaaS-Daten angemessene technische und organisatorische Massnahmen zu treffen. arteria implementiert insbesondere Zugangskontrollen, Zugriffskontrollen sowie Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Massnahmen. Bei der Auswahl der Massnahmen berücksichtigt arteria den Stand der Technik, die Implementierungskosten sowie die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für betroffene Personen. Die jeweils geltenden Massnahmen ergeben sich aus den aktuellen Leistungsbeschrieben von arteria.

6.5. arteria verpflichtet sich, den Kunden ohne Verzug schriftlich zu informieren, wenn arteria Kenntnis von einer Datensicherheits-Verletzung erlangt, die personenbezogene SaaS-Daten betrifft. Dabei hat arteria dem Kunden die Art und das Ausmass der Verletzung sowie mögliche Abhilfemassnahmen mitzuteilen. Die Vertragsparteien treffen gemeinsam die erforderlichen Massnahmen, um den Schutz der personenbezogenen SaaS-Daten sicherzustellen und mögliche nachteilige Folgen für die betroffenen Personen zu mildern. Überdies verpflichtet sich arteria, dem Kunden auf schriftliche Anfrage ausreichende Informationen zur Verfügung zu stellen, damit dieser seinen Pflichten gemäss EU-DSGVO oder anderen anwendbaren Datenschutzgesetzen betreffend die Meldung, Untersuchung und Dokumentation von Datensicherheits-Verletzungen erfüllen kann.

6.6. arteria verpflichtet sich, den Kunden auf schriftliche Anfrage und gegen separate angemessene Vergütung sowie im Rahmen der betrieblichen Ressourcen und Möglichkeiten von arteria bei der Erfüllung von Betroffenenrechten (insbesondere Auskunfts-, Berichtigungs- und Löschungsrechten) durch den Kunden (personenbezogene SaaS-Daten betreffend) gemäss Kapitel III der EU-DSGVO (oder äquivalenten Bestimmunen anderer anwendbarer Datenschutzgesetze) zu unterstützen. Richtet sich eine betroffene Person mit Forderungen betreffend die Erfüllung von Betroffenenrechten direkt an arteria,

wird arteria die betroffene Person an den Kunden verweisen. Voraussetzung dafür ist, dass arteria eine solche Zuordnung an den Kunden gestützt auf die Angaben der betroffenen Person vornehmen kann.

6.7. arteria ist verpflichtet, den Kunden ohne Verzug schriftlich zu benachrichtigen, wenn arteria eine Anfrage (z.B. ein Auskunfts- oder Löschungsbegehren) von einer betroffenen Person in Bezug auf personenbezogene SaaS-Daten erhält; vorausgesetzt eine Zuordnung an den Kunden ist gestützt auf die Angaben der betroffenen Person möglich.

6.8. arteria ist auf schriftliche Anfrage und gegen separate angemessene Vergütung sowie unter Berücksichtigung der betrieblichen Ressourcen und Möglichkeiten von arteria bereit, den Kunden bei Datenschutz-Folgenabschätzungen und bei Konsultationen der Aufsichtsbehörden zu unterstützen.

6.9. arteria wird die personenbezogenen SaaS-Daten nach Ende der Laufdauer des SaaS-Vertrags gemäss den Bestimmungen des SaaS-Vertrags herausgeben oder löschen.

7. Beizug von Unter-Auftragsverarbeitern

7.1. Beansprucht der Kunde Dienstleistungen von arteria, die personenbezogene SaaS-Daten betreffen und durch Dritte erbracht werden, bleibt arteria gegenüber dem Kunden Auftragsverarbeiter und erfüllt die diesbezüglichen Pflichten aus dem AVV. Der Anbieter der Drittdienstleistung, die in der Dienstleistung von arteria integriert wird, ist Unter-Auftragsverarbeiter von arteria. Davon zu unterscheiden sind Fälle, in denen arteria dem Kunden einen direkten Vertragsschluss mit dem Drittdienstleister vermittelt und der Drittdienstleister direkt Auftragsverarbeiter des Kunden wird. In solchen Fällen hat der Kunde selber dafür besorgt zu sein, unter anwendbaren Datenschutzgesetzen allenfalls notwendige Vereinbarungen mit dem Drittdienstleister zu treffen.

7.2. arteria ist berechtigt, Unter-Auftragsverarbeiter im Rahmen der Erbringung der SaaS-Dienstleistungen von arteria beizuziehen. arteria ist in solchen Fällen verpflichtet, mit Unter-Auftragsverarbeitern im erforderlichen Umfang eine Vereinbarung zu treffen, die arteria die Einhaltung der Bestimmungen diesem AVV ermöglicht.

7.3. arteria wird den Kunden vorab in geeigneter Weise informieren, wenn arteria nach Inkrafttreten dieses AVV in Bezug auf bestehende SaaS-Dienstleistungen neue Unter-Auftragsverarbeiter beizieht oder bestehende austauscht. Wenn der Kunde dem nicht innerhalb von dreissig (30) Tagen nach dem Datum der Mitteilung aus wichtigen datenschutzrechtlichen Gründen widerspricht, gilt der neue oder ausgetauschte Unter-Auftragsverarbeiter als genehmigt.

7.4. Wenn die Unter-Auftragsverarbeitung eine Übermittlung von personenbezogenen SaaS-Daten in ein Land ausserhalb des Gebiets der EU/EWR/Schweiz beinhaltet, stellt arteria sicher, dass arteria die Bestimmungen der EU-DSGVO (oder ähnlicher Bestimmungen des Schweizer DSG) betreffend die Datenübermittlung in ein Drittland einhält (z.B. durch Auswahl eines Unter-Auftragsverarbeiters, der dem U.S.-Swiss Privacy Shield unterstellt ist, oder durch Miteinbezug anerkannter Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländer).

8. Pflichten des Kunden

8.1. Der Kunde ist für die Rechtmässigkeit der Verarbeitung der personenbezogenen SaaS-Daten, einschliesslich der Zulässigkeit der Auftrags- bzw. Unter-Auftragsverarbeitung, verantwortlich.

8.2. Der Kunde trifft in seinem Verantwortungsbereich (z.B. auf seinen eigenen Systemen und Applikationen) selbstständig angemessene technische und organisatorische Massnahmen zum Schutz der personenbezogenen SaaS-Daten.

8.3. Der Kunde verpflichtet sich, arteria unverzüglich zu informieren, wenn der Kunde in der Leistungserbringung von arteria Verletzungen von anwendbaren Datenschutzgesetzen feststellt.

9. Informations- und Prüfungsrechte

9.1. arteria ist verpflichtet, dem Kunden auf schriftliche Anfrage alle Informationen zur Verfügung zu stellen, die dieser vernünftigerweise zum Nachweis der Einhaltung dieses AVV gegenüber betroffenen Personen oder Datenschutzaufsichtsbehörden benötigt.

9.2. arteria ermöglicht dem Kunden oder einem vom Kunden beauftragten und zur Vertraulichkeit verpflichteten Prüfer, die Einhaltung dieses AVV durch arteria zu prüfen. Werden nach Vorlage

entsprechender Nachweise Verletzungen des AVV durch arteria festgestellt, hat arteria unverzüglich und kostenlos geeignete Korrekturmassnahmen zu implementieren.

9.3. Die vorstehenden Informations- und Prüfungsrechte des Kunden bestehen nur insoweit, als der SaaS-Vertrag dem Kunden keine anderen Informations- und Prüfungsrechte einräumt, die den einschlägigen Anforderungen der anwendbaren Datenschutzgesetze entsprechen. Weiter stehen diese Informations- und Prüfungsrechte unter dem Vorbehalt des Verhältnismässigkeitsgebots und der Wahrung der schutzwürdigen Interessen (insbesondere Sicherheits- oder Geheimhaltungsinteressen) von arteria. Vorbehältlich einer anderslautenden Vereinbarung zwischen den Vertragsparteien trägt der Kunde sämtliche Kosten der Information und Prüfung, einschliesslich nachgewiesener interner Kosten von arteria.

10. Änderungen dieses AVV

10.1. arteria behält sich vor, diesen AVV zu ändern, (a) wenn dies zur Anpassung an Rechtsentwicklungen erforderlich ist oder (b) wenn dies nicht zu einer Verschlechterung der Gesamtsicherheit der Auftragsverarbeitung führt und sich (nach Ermessen von arteria) nicht erheblich nachteilig auf die Rechte der von der Auftragsverarbeitung betroffenen Personen auswirkt.

10.2. arteria teilt dem Kunden beabsichtigte Änderungen dieses AVV gemäss Ziff. 10.1 spätestens dreissig (30) Tage vor Wirksamwerden mit. Wenn der Kunde der Änderung widersprechen möchte, kann er den AVV innerhalb von dreissig (30) Tagen ab Datum der Mitteilung in der Administrationsoberfläche kündigen. Ohne Widerspruch innerhalb dieser Frist gilt die Änderung als genehmigt.

11. Generelle Bestimmungen

11.1. In Abweichung allfälliger im SaaS-Vertrag vereinbarter Schriftformvorbehalte kann der AVV auf elektronischem Weg zwischen den Vertragsparteien vereinbart oder geändert werden.

11.2. Verlangt dieser AVV eine schriftliche Aufforderung oder Mitteilung, so genügt (für Mitteilungen an den Kunden) E-Mail an die bei arteria bekannte Adresse des Kunden bzw. (für Mitteilungen an arteria) E-Mail an info@arteria.ch dem Schriftformerfordernis.

11.3. Datenschutzrechtliche Begriffe wie "personenbezogene Daten", "verarbeiten", "Verantwortlicher", "Auftragsverarbeiter", "Datenschutz-Folgenabschätzung", etc. haben die ihnen in der EU-DSGVO oder, je nach Kontext, im Schweizer DSG zugeschriebene Bedeutung. "Datensicherheits-Verletzung" meint "Verletzung des Schutzes personenbezogener Daten" (englisch: "Personal Data Breach").

11.4. Die Vertragsparteien unterwerfen sich hiermit der im SaaS-Vertrag festgelegten Gerichtsstands-Wahl für sämtliche Streitigkeiten sowie Ansprüche aus oder im Zusammenhang mit diesem AVV.

11.5. Sollten einzelne oder mehrere Bestimmungen des AVV unwirksam oder nichtig sein oder werden, berührt dies die Wirksamkeit der übrigen Bestimmungen nicht. An die Stelle der unwirksamen oder nichtigen Bestimmungen tritt diejenige Regelung, welche die Vertragsparteien bei Kenntnis des Mangels zum Zeitpunkt des Abschlusses des AVV nach Treu und Glauben sowie nach wirtschaftlicher Betrachtungsweise getroffen hätten. Entsprechendes gilt im Fall etwaiger Lücken des AVV.