Vereinbarung zur Verarbeitung personenbezogener Daten im Auftrag

[Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679 (DS-GVO]

Im Rahmen der zwischen atmio und dem im Auftrag genannten Partner geschlossenen Vereinbarung verarbeiten wir personenbezogene Daten im Auftrag des jeweiligen Partners. Zum Schutz personenbezogener Daten sind wir gesetzlich verpflichtet, detailliert zu dokumentieren, welche Maßnahmen wir zum Schutz dieser Daten ergreifen, dass wir die Erfassung der Daten auf ein Minimum begrenzen und diese umgehend wieder löschen, wenn sie nicht mehr benötigt werden.

Die vorliegende Vereinbarung zur Verarbeitung personenbezogener Daten im Auftrag und ihre Anhänge [abrufbar unter https://www.atmio.com/vertrag enthält die Vereinbarung zwischen dem Partner und atmio betreffend die Verarbeitung personenbezogener Daten durch atmio. Sie ergänzt die bestehenden Vereinbarungen, in denen auf sie verwiesen wird, und ist ein integraler Bestandteil derselben. Sie wird zwischen dem Partner und atmio verbindlich, sobald sie in die Vereinbarung aufgenommen wurde. Im Falle von Widersprüchen hat diese Vereinbarung zur Verarbeitung personenbezogener Daten im Auftrag und ihre Anhänge Vorrang vor den sonstigen Bestimmungen der Vereinbarung.

Wenn Sie diese Vereinbarung zur Verarbeitung personenbezogener Daten im Auftrag und ihre Anhänge separat unterzeichnen möchten, können Sie unter https://www.atmio.com/vertrag eine bereits von atmio unterzeichnete Version herunterladen. Oder sprechen Sie Ihren Kontakt bei atmio direkt an.

Dies vorweggeschickt, vereinbaren die Parteien, was folgt:

ABSCHNITT I

Klausel 1

Zweck und Anwendungsbereich

a) Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) soll die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG sichergestellt werden.

b) Die in Anhang I aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 und/oder Artikel 29 Absätze 3 und 4 der Verordnung (EU) 2018/1725 zu gewährleisten.

c) Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß Anhang II.

d) Die Anhänge I bis IV sind Bestandteil der Klauseln.

e) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

f) Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 erfüllt werden.

Klausel 2

Unabänderbarkeit der Klauseln

a) Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.

b) Dies hindert die Parteien nicht daran die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

Klausel 3

Auslegung

a) Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.

b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 auszulegen.

c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

Klausel 4

Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

Klausel 5

[bewusst leer]

ABSCHNITT II – PFLICHTEN DER PARTEIEN

Klausel 6

Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in Anhang II aufgeführt.

Klausel 7

Pflichten der Parteien

7.1 Weisungen

a) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.

b) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679, die Verordnung (EU) 2018/1725 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

7.2 Zweckbindung

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Anhang II genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

7.3 Dauer der Verarbeitung personenbezogener Daten

Die Daten werden vom Auftragsverarbeiter nur für die in Anhang II angegebene Dauer verarbeitet.

7.4 Sicherheit der Verarbeitung

a) Der Auftragsverarbeiter ergreift mindestens die in Anhang III aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.

b) Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7.5 Sensible Daten

Falls die Verarbeitung personenbezogene Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten"), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

7.6 Dokumentation und Einhaltung der Klauseln

a) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.

b) Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.

d) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.

e) Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

7.7 Einsatz von Unterauftragsverarbeitern

a) Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens 14 Tage im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

b) Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den

Auftragsverarbeiter gemäß diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesen Klauseln und gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

d) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

e) Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche – im Falle, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

7.8 Internationale Datenübermittlungen

a) Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 im Einklang stehen.

b) Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 7.7 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

Klausel 8

Unterstützung des Verantwortlichen

a) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.

b) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung

ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.

c) Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 8 Buchstabe b zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:

1) Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung"), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;

2) Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;

3) Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;

4) Verpflichtungen gemäß Artikel 32 der Verordnung (EU) 2016/679.

d) Die Parteien legen in Anhang III die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

Klausel 9

Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 oder gegebenenfalls den Artikeln 34 und 35 der Verordnung (EU) 2018/1725 nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

9.1 Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

a) bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);

b) bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der Verordnung (EU) 2016/679 in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:

1) die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

2) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

3) die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt;

c) bei der Einhaltung der Pflicht gemäß Artikel 34 der Verordnung (EU) 2016/679, die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

9.2 Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

a) eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);

b) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;

c) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

Die Parteien legen in Anhang III alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Artikel 33 und 34 der Verordnung (EU) 2016/679 zu unterstützen.

ABSCHNITT III – SCHLUSSBESTIMMUNGEN

Klausel 10

Verstöße gegen die Klauseln und Beendigung des Vertrags

a) Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.

b) Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn

1) der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;

2) der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 nicht erfüllt;

3) der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 zum Gegenstand hat, nicht nachkommt.

c) Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 7.1 Buchstabe b verstoßen.

d) Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

ANHANG I – LISTE DER PARTEIEN

Verantwortliche(r): [Name und Kontaktdaten des/der Verantwortlichen und gegebenenfalls des Datenschutzbeauftragten des Verantwortlichen]

Ist das in der zugrundeliegenden Vereinbarung als „Partner“ bezeichnete Unternehmen, für das diese Vereinbarung zur Verarbeitung personenbezogener Daten im Auftrag und ihre Anhänge mit Unterzeichnung der zugrundeliegenden Vereinbarung verbindlich wird.

Auftragsverarbeiter: [Name und Kontaktdaten des/der Auftragsverarbeiter/s und gegebenenfalls des Datenschutzbeauftragten des Auftragsverarbeiters]

M2Tech GmbH, Stadtdeich 2, c/o Factory Hammerbrooklyn, 20097 Hamburg

Name, Funktion und Kontaktdaten der Kontaktperson:
Marius Krüger, Geschäftsführer, marius@atmio.com, +49 151 61 40 92 48

Für die M2Tech GmbH wird diese Vereinbarung zur Verarbeitung personenbezogener Daten im Auftrag und ihre Anhänge mit Unterzeichnung der zugrundeliegenden Vereinbarung verbindlich.

ANHANG II – BESCHREIBUNG DER VERARBEITUNG

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden:
Nutzer der atmio-App und der atmio-Software, Mitarbeitende des Verantwortlichen, Kunden des Verantwortlichen.

Kategorien personenbezogener Daten, die verarbeitet werden:
Nutzerdaten, Standortdaten, Nutzungsdaten.

Verarbeitete sensible Daten (falls zutreffend) und angewandte Beschränkungen oder Garantien, die der Art der Daten und den verbundenen Risiken in vollem Umfang Rechnung tragen, z. B. strenge Zweckbindung, Zugangsbeschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen oder zusätzliche Sicherheitsmaßnahmen:
n.a.

Art der Verarbeitung

- Speichern
- Auslesen
- Abfragen
- Löschen
- Organisieren/Ordnen

Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden: Betrieb und Nutzung der atmio-Lösungen des Verantwortlichen, Support, Wiederherstellen der Funktionsfähigkeit des Systems, Aktualisierungen der atmio-Software bzw. atmio-App.

Die Dauer der Verarbeitung richtet sich nach den Bestimmungen des zwischen den Parteien auf Grundlage des atmio-Angebots abgeschlossenen Auftrags, der als Leistungsvereinbarung zwischen den Parteien abgeschlossen wird.

ANHANG III – TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN, EINSCHLIESSLICH ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN

Gemäß Art. 32 DSGVO sind unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen durch den Verantwortlichen und den Auftragsverarbeiter geeignete technisch-organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.
Bei Datenübermittlungen an Unterauftragsverarbeiter sind auch die spezifischen technischen und organisatorischen Maßnahmen zu beschreiben, die der Unterauftragsverarbeiter zur Unterstützung des Verantwortlichen ergreifen muss.

Beschreibung der von dem Auftragnehmer ergriffenen technischen und organisatorischen Sicherheitsmaßnahmen:

1. Maßnahmen zur Pseudonymisierung und Verschlüsselung personenbezogener Daten

Anforderung
Pseudonymisierung: Unter Pseudonymisierung versteht man die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten nicht mehr einer bestimmten Person direkt zugeordnet werden können. Die Identifikationsmerkmale werden durch ein Pseudonym ersetzt, so dass eine Re-Identifizierung grundsätzlich möglich ist. Pseudonymisierung ist ein wichtiges Instrument, um Datenschutz zu gewährleisten. Bei einem unbefugten Zugriff Dritter auf pseudonymisierte Daten, besteht ein geringeres Risiko, da das Pseudonym nicht einfach einer identifizierbaren Person zugeordnet werden kann. Verschlüsselung: Unter Verschlüsselung versteht man den Einsatz kryptographischer Verfahren, so dass personenbezogene Daten für unbefugte Dritte unleserlich und unverständlich werden.

Maßnahmen zur Umsetzung	
☒ Transportverschlüsselung von E-Mails (TLS)	

2. Verfahren zur Gewährleistung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung

2.1 Zugangs-, Zutritts- und Zugriffskontrolle sowie Eingabekontrolle

Anforderung

Es müssen Vorkehrungen getroffen werden, um zu verhindern, dass Unbefugte Zugriff auf Datenverarbeitungsanlagen erhalten, die personenbezogene Daten verarbeiten. Ebenso muss sichergestellt werden, dass Unbefugte die Datenverarbeitungssysteme nicht nutzen können und keinen physischen Zugang zu den Räumlichkeiten haben, in denen IT-Systeme betrieben und genutzt werden. Des Weiteren müssen Maßnahmen ergriffen werden, um sicherzustellen, dass nur autorisierte Personen auf die personenbezogenen Daten zugreifen können, für die sie Zugriffsberechtigung haben. Dies gewährleistet, dass diejenigen, die die Datenverarbeitungsverfahren nutzen dürfen, ausschließlich auf die dafür vorgesehenen personenbezogenen Daten zugreifen können. Es sind unter anderem die Maßnahmen zur Identifizierung und Autorisierung der Nutzer sowie zur Gewährleistung der physischen Sicherheit von Orten, an denen personenbezogene Daten verarbeitet werden, zu nennen. Zudem sind Maßnahmen zum Schutz der Daten während der Übermittlung und Speicherung aufzuführen.

Maßnahmen zur Umsetzung	
☒ Rechner verfügen über individuelle, personenbezogene Benutzerkennungen	☒ Server verfügen über individuelle Benutzerkennungen
☒ Zwei-Faktor-Authentisierung	☒ Automatisierte Sperrung bei Inaktivität des PCs
☒ Der Zugang zum System wird bei mehrfacher fehlerhafter Eingabe des Passwortes gesperrt	☒ Begrenzte Administratoren-Anzahl
☒ Schließanlage der Eingangstüren	☒ Administratorrechte sind definiert
☒ Der Zutritt von Reinigungs- und Wartungspersonal zum Gebäude ist geregelt	☒ Der Zutritt und Aufenthalt von Besuchern erfolgt in Begleitung von Firmenpersonal

2.2 Belastbarkeit der Systeme

Anforderung
Der Begriff "Belastbarkeit" oder "Resilienz" bezeichnet die Fähigkeit eines Unternehmens, auch bei Störungen und Eingriffen weiterhin bestehen und funktionieren zu können, ohne dabei erheblichen Schaden zu nehmen. Dies umfasst unter anderem die Implementierung gängiger IT-Schutzmaßnahmen. Aufgeführt werden Maßnahmen zur Gewährleistung der Protokollierung von Ergebnissen, für die interne Governance und Verwaltung der IT- und IT-Sicherheit, zur Gewährleistung der Systemkonfiguration, einschließlich der Standardkonfiguration und zur Zertifizierung/ Qualitätssicherung von Prozessen und Produkten.

Maßnahmen zur Umsetzung	
☒ Datensicherheitskonzept vorhanden	☒ Revisionsfestigkeit der Daten
☒ Incident Management	☒ Patch-Management

☒ Aktuelle Backuplösungen	☒ Datensicherheitskonzepte

3. Maßnahmen zur Sicherstellung der Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen

Anforderung	
Maßnahmen, die sicherstellen sollen, dass die eingesetzten Systeme nach einem physischen oder technischen Störungsfall wiederhergestellt werden können. Maßnahmen zur Gewährleistung einer begrenzten Vorratsdatenspeicherung, zur Ermöglichung der Datenübertragbarkeit.	
Maßnahmen zur Umsetzung	
☒ Datenbackupkonzepte	☒ Incidentmanagement
☒ Nutzung unterschiedlicher Datenbanken	☒ Physische oder technische Dateientrennung

4. Verfahren, die der regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung dienen.

Anforderung	
Die vorgenannten Maßnahmen reichen nicht aus, um ein angemessenes Schutzniveau zu gewährleisten, da sich die Risiken verändern und fortlaufend neue Gefahren entstehen. Ein angemessenes Schutzniveau kann daher nur durch einen fortlaufenden Prozess der Überprüfung, Bewertung und Evaluierung sichergestellt werden. Maßnahmen zur Gewährleistung der Rechenschaftspflicht.	
Maßnahmen zur Umsetzung	
☐ Externe Anbieter prüfen die Wirksamkeit der Maßnahmen	☒ Interne Prüfzyklen innerhalb derer eine Revision der technischen und organisatorischen Maßnahmen erfolgt

5. Verfahren zur Gewährleistung, dass Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten

Anforderung
Es müssen Vorkehrungen getroffen werden, um sicherzustellen, dass personenbezogene Daten, die

vom Auftraggeber übermittelt werden, nur gemäß seinen Anweisungen verarbeitet werden.	
Maßnahmen zur Umsetzung	
☒ Regelmäßige Datenschutzschulungen der Mitarbeiter	☒ Dokumentierte Weisungen des Auftraggebers

Beschreibung der von technischen und organisatorischen Sicherheitsmaßnahmen, die die vom Auftragnehmer eingesetzten Unterauftragsverarbeiter (Anhang IV) ergriffen haben:

Amazon Web Services EMEA SARL (etwaige Änderungen und Ergänzungen sind jederzeit online abrufbar unter https://d1.awsstatic.com/legal/aws-dpa/aws-dpa.pdf):

Security Standards

Capitalized terms not otherwise defined in this document have the meanings assigned to them in the Agreement.

1 Information Security Program. AWS will maintain an information security program designed to (a) enable Customer to secure Customer Data against accidental or unlawful loss, access, or disclosure, (b) identify reasonably foreseeable risks to the security and availability of the AWS Network, and (c) minimize physical and logical security risks to the AWS Network, including through regular risk assessment and testing. AWS will designate one or more employees to coordinate and be accountable for the information security program.

AWS's information security program will include the following measures:

1.1 Logical Security.

A. Access Controls. AWS will make the AWS Network accessible only to authorized personnel, and only as necessary to maintain and provide the Services. AWS will maintain access controls and policies to manage authorizations for access to the AWS Network from each network connection and user, including through the use of firewalls or functionally equivalent technology and authentication controls. AWS will maintain access controls designed to (i) restrict unauthorized access to data, and

(ii) segregate each customer's data from other customers' data.

B. Restricted User Access. AWS will (i) provision and restrict user access to the AWS Network in accordance with least privilege principles based on personnel job functions, (ii) require review and approval prior to provisioning access to the AWS Network above least privileged principles, including administrator accounts; (iii) require at least quarterly review of AWS Network access privileges and, where necessary, revoke AWS Network access privileges in a timely manner, and (iv) require two- factor authentication for access to the AWS Network from remote locations.

C. Vulnerability Assessments. AWS will perform regular external vulnerability assessments and penetration testing of the AWS Network, and will investigate identified issues and track them to resolution in a timely manner.

D. Application Security. Before publicly launching new Services or significant new features of Services, AWS will perform application security reviews designed to identify, mitigate and remediate security risks.

E. Change Management. AWS will maintain controls designed to log, authorize, test, approve and document changes to existing AWS Network resources, and will document change details within its change management or deployment tools. AWS will test changes according to its change management standards prior to migration to production. AWS will maintain processes designed to detect unauthorized changes to the AWS Network and track identified issues to a resolution.

F. Data Integrity. AWS will maintain controls designed to provide data integrity during transmission, storage and processing within the AWS Network. AWS will provide Customer the ability to delete Customer Data from the AWS Network.

G. Business Continuity and Disaster Recovery. AWS will maintain a formal risk management program designed to support the continuity of its critical business functions ("Business Continuity Program"). The Business Continuity Program includes processes and procedures for identification of, response to, and recovery from, events that could prevent or materially impair AWS's provision of the Services (a

"BCP Event"). The Business Continuity Program includes a three-phased approach that AWS will follow to manage BCP Events:

(i) Activation & Notification Phase. As AWS identifies issues likely to result in a BCP Event, AWS will escalate, validate and investigate those issues. During this phase, AWS will analyze the root cause of the BCP Event.

(ii) Recovery Phase. AWS assigns responsibility to the appropriate teams to take steps to restore normal system functionality or stabilize the affected Services.

(iii) Reconstitution Phase. AWS leadership reviews actions taken and confirms that the recovery effort is complete and the affected portions of the Services and AWS Network have been restored. Following such confirmation, AWS conducts a post-mortem analysis of the BCP Event.

H. Incident Management. AWS will maintain corrective action plans and incident response plans to respond to potential security threats to the AWS Network. AWS incident response plans will have defined processes to detect, mitigate, investigate, and report security incidents. The AWS incident response plans include incident verification, attack analysis, containment, data collection, and problem remediation. AWS will maintain an AWS Security Bulletin (as of the Effective Date, http://aws.amazon.com/security/security-bulletins/) which publishes and communicates security related information that may affect the Services and provides guidance to mitigate the risks identified.

I. Storage Media Decommissioning. AWS will maintain a media decommissioning process that is conducted prior to final disposal of storage media used to store Customer Data. Prior to final disposal, storage media that was used to store Customer Data will be degaussed, erased, purged, physically destroyed, or otherwise sanitized in accordance with industry standard practices designed to ensure that the Customer Data cannot be retrieved from the applicable type of storage media.

1.2 Physical Security.

A. Access Controls. AWS will (i) implement and maintain physical safeguards designed to prevent unauthorized physical access, damage, or interference to the AWS Network, (ii) use appropriate control devices to restrict physical access to the AWS Network to only authorized personnel who have a legitimate business need for such access, (iii) monitor physical access to the AWS Network using intrusion detection systems designed to monitor, detect, and alert appropriate personnel of security incidents, (iv) log and regularly audit physical access to the AWS Network, and (v) perform periodic reviews to validate adherence with these standards.

B. Availability. AWS will (i) implement redundant systems for the AWS Network designed to minimize the effect of a malfunction on the AWS Network, (ii) design the AWS Network to anticipate and tolerate hardware failures, and (iii) implement automated processes designed to move customer data traffic away from the affected area in the case of hardware failure.

1.3 AWS Employees.

A. Employee Security Training. AWS will implement and maintain employee security training programs regarding AWS information security requirements. The security awareness training programs will be reviewed and updated at least annually.

B. Background Checks. Where permitted by law, and to the extent available from applicable governmental authorities, AWS will require that each employee undergo a background investigation

that is reasonable and appropriate for that employee's position and level of access to the AWS Network.

2 Continued Evaluation. AWS will conduct periodic reviews of the information security program for the AWS Network. AWS will update or alter its information security program as necessary to respond to new security risks and to take advantage of new technologies.

AWS Certifications and Audits.

10.1 AWS ISO-Certification and SOC Reports. In addition to the information contained in this DPA, upon Customer's request, and provided that the parties have an applicable NDA in place, AWS will make available the following documents and information: (i) the certificates issued for the ISO 27001 certification, the ISO 27017 certification, the ISO 27018 certification, and the ISO 27701 certification (or the certifications or other documentation evidencing compliance with such alternative standards as are substantially equivalent to ISO 27001, ISO 27017, ISO 27018, and ISO 27701); and (ii) the System and Organization Controls (SOC) 1 Report, the System and Organization Controls (SOC) 2 Report and the System and Organization Controls (SOC) 3 Report (or the reports or other documentation describing the controls implemented by AWS that replace or are substantially equivalent to the SOC 1, SOC 2 and SOC 3).

10.2 AWS Audits. AWS uses external auditors to verify the adequacy of its security measures, including the security of the physical data centers from which AWS provides the Services. This audit: (a) will be performed at least annually; (b) will be performed according to ISO 27001 standards or such other alternative standards that are substantially equivalent to ISO 27001; (c)

will be performed by independent third-party security professionals at AWS's selection and expense; and (d) will result in the generation of an audit report ("Report"), which will be AWS's Confidential Information.

10.3 Audit Reports. At Customer's written request, and provided that the parties have an applicable NDA in place, AWS will provide Customer with a copy of the Report so that Customer can reasonably verify AWS's compliance with its obligations under this DPA.

Atlassian Pty Ltd (Stand 07.10.2025; etwaige Änderungen und Ergänzungen sind jederzeit online abrufbar unter https://www.atlassian.com/legal/security-measures#acesss-control):

Introduction

Security is an essential part of Atlassian's offerings. This page describes Atlassian's security program, certifications, policies, and physical, technical, organizational and administrative controls and measures to protect Customer Data and, where indicated below, Customer Materials from unauthorized access, destruction, use, modification or disclosure (the "Security Measures"). The Security Measures are consistent with the commonly-accepted industry standards and practices, including NIST 800-53 controls.

Any capitalized terms used but not defined have the meanings set out in the Agreement or the Data Processing Addendum. Further details on Atlassian's security posture can be found in our Trust Center and Compliance Resource Center.

1. Access Control

Atlassian maintains a comprehensive set of formal policies, controls, and practices for the appropriate access control when processing Customer Data and Customer Materials, which includes:

1.1. access management policy addressing access control standards, including the framework and the principles for user provisioning;

1.2. designated criticality tiers based on a Zero Trust Model architecture, including the requirements for multi-factor authentication on higher-tier services;

1.3. user provisioning for access to Atlassian systems, applications and infrastructure based on the relevant job role and on the least privilege principle that is enforced through the authentication processes, enabling only authorized personnel to have access to development and build environments (including source code repositories) associated with the Products;

1.4. strict role-based access controls for Atlassian staff, allowing access to Customer Data only on a need-to-know basis;

1.5. segregation of duties including but not limited to (i) access controls reviews, (ii) HR-application managed security groups, and (iii) workflow controls;

1.6. a prior approval of all user accounts by Atlassian's management before granting access to data, applications, infrastructure, or network components based on the data classification level; regular review of access rights as required by relevant role;

1.7. use of technical controls such as virtual private network (VPN) and multi-factor authentication (MFA) where relevant based on information classification and Atlassian's Zero Trust Model architecture;

1.8. centrally managed mobile device management (MDM) solution, including defined lockout periods and posture checks for endpoints and mobile devices;

1.9. identifying and removing redundant and dormant accounts, promptly revoking access through automated and regular review processes.

2. Awareness and Training

Atlassian maintains a comprehensive set of formal policies, controls, and practices for conducting appropriate trainings and security awareness activities, which includes:

2.1. extensive awareness training on security, privacy, and compliance topics for all employees at induction and annually, utilizing diverse formats (online, in-person, and pre-recorded sessions, phishing simulations);

2.2. targeted role-specific training and documentation for employees with elevated privileges to address relevant risks and enhance their specific knowledge as required for their respective roles;

2.3. maintaining all training records in a designated learning management system;

2.4. an automated reminder for training deadlines, with a built-in escalation process to respective managers;

2.5. continuous security awareness trainings (extending to contractors and partners), covering current threats and best security practices;

2.6. secure coding trainings by security champions embedded within engineering teams;

2.7. annual mandatory security trainings and events to reinforce security principles through different activities, emphasizing the collective responsibility for security;

2.8. annual secure development training to Atlassian developers in alignment with industry standards.

3. Audit and Accountability

Atlassian maintains a comprehensive set of formal policies, controls, and practices for proper auditing and accountability purposes, which includes:

3.1. comprehensive logging standards as part of Atlassian's policy management framework, with annual reviews and senior management approvals;

3.2. secure forwarding and storage of relevant system logs to a centralized log platform of the cloud infrastructure with read-only access;

3.3. monitoring of security audit logs to detect unusual activity, with established processes for reviewing and addressing anomalies;

3.4. regular updates to the logging scope of information and system events for Cloud Products and related infrastructure in order to address new features and changes;

3.5. utilizing time sync services from relevant cloud service providers (e.g. AWS or Microsoft Azure) for reliable timekeeping across all deployed instances.

4. Assessment, Authorisation and Monitoring

Atlassian maintains a comprehensive set of formal policies, controls, and practices for consistent system monitoring and security assessments, which includes:

4.1. extensive audit and assurance policies with annual reviews and updates;

4.2. a centralized internal policy program categorising the global policies into different domains including annual review, and senior management approval of the program;

4.3. audit management encompassing the planning, risk analysis, security control assessment, conclusion, remediation schedules, and review of past audit reports;

4.4. internal and independent external audits conducting annual evaluations of legal and contractual requirements, as well as effectiveness of controls and processes to validate compliance;

4.5. ongoing verification of compliance against relevant standards and regulations, e.g. ISO 27001 or SOC 2;

4.6. systematically addressing any nonconformities found through audit findings taking into account the root-cause analysis, severity rating, and corrective actions;

4.7. annual penetration testing on Cloud and Software Products and proactive bug bounty programs for the detection and mitigation of vulnerabilities;

4.8. continuous vulnerability scanning consistent with commonly-accepted standards and practices for security testing with subsequent remediation of identified vulnerabilities based on the Common Vulnerability Scoring System (CVSS) in line with Atlassian's Security Bugfix Policy;

4.9. security testing, privacy risk and vulnerability assessments of the relevant Cloud Products and processes at least annually.

5. Configuration Management

Atlassian maintains a comprehensive set of formal policies, controls, and practices for appropriate configuration management, which includes:

5.1. change management policies covering the risk management for all internal and external asset changes, reviewed annually;

5.2. standard procedures for change management applicable to encryption and cryptography for the secure handling of data (e.g. encryption keys) according to its security classification, including but not limited to key rotation, defining key ownership, secure storage;

5.3. a centralized internal policy program categorising the global policies into different domains including annual review, and senior management approval of the program;

5.4. stringent policies encompassing (i) encryption, (ii) cryptography, (iii) endpoint management, and (iv) asset tracking inline with industry standards;

5.5. established baselines and standards for change control that require testing documentation prior to implementation and authorized approval;

5.6. a peer review and green build process requiring multiple reviews and successful testing for production code and infrastructure changes;

5.7. a strict post-implementation testing and approval process for emergency changes to the code;

5.8. comprehensive automated system supplemented by an Intrusion Detection System (IDS), managing and protecting against unauthorized changes;

5.9. cataloguing and tracking of all physical and logical assets with annual reviews ensuring up-to-date asset management;

5.10. continuous monitoring and managing the health (including capacity) and availability of assets and Cloud Products, including their underlying components.

6. Contingency Planning

Atlassian maintains a comprehensive set of formal policies, controls, and practices for appropriate contingency planning for business continuity and disaster recovery purposes, which includes:

6.1. a skilled workforce and robust IT infrastructure, including telecommunications and technology essential for Product delivery;

6.2. business continuity and disaster recovery plans ("BCDR Plans"), including defined recovery time objectives (RTOs) and recovery point objectives (RPOs);

6.3. business continuity plans encompassing data storage and continuity of use, reasonably designed to prevent interruption to access and utilization;

6.4. geographic diversity as a result of our global workforce and cloud infrastructure;

6.5. reinforcing business operations through resilience controls, such as daily backups, annual restoration testing, and alternative cloud infrastructure storage sites;

6.6. a resilience framework and procedures for response and remediation of cybersecurity events in order to maintain business continuity;

6.7. quarterly disaster recovery tests and exercises to enhance response strategies, with post-test analyses for continuous improvement aligned with applicable BCDR Plans;

6.8. continuous capacity management across Cloud Products, with internal monitoring and adjustments to maintain service availability and processing capacity, for example distributed denial-of-service attack (DDoS) mitigation for Cloud Products and related infrastructure;

6.9. a centralized internal policy program for annual reviews and updates of all global policies related to business continuity;

6.10. robust backup protocols, including (i) data encryption, (ii) redundancy across data centers, and (iii) regular testing to bolster contingency planning.

7. Identification and Authentication

Atlassian maintains a comprehensive set of formal policies, controls, and practices for appropriate identification and authentication purposes which includes:

7.1. employee identification uniquely through active directory, utilising single sign-on (SSO) for application access;

7.2. utilising of MFA for secure access, specifically for VPN and application launch via SSO based on Atlassian's Zero Trust Model architecture;

7.3. password policies following the NIST 800-63B guidelines, focusing on the security aspects of password creation and management;

7.4. ensuring the security of stored credentials using advanced encryption methods, e.g. password and secret management systems;

7.5. documented approvals, regular reviews of users and accounts, and automatic syncs between the relevant identity system and human resources systems to maintain the integrity and accuracy of identification data.

8. Security Incident Response

Atlassian maintains a comprehensive set of formal policies, controls, and practices for appropriate Security Incident response purposes, which includes:

8.1. security Incident response plans emphasizing preparedness, containment, eradication and recovery, as well as focus on data protection and other regulatory requirements;

8.2. dedicated cross-functional teams handling Security Incidents, ensuring effective communication and collaboration, including well-defined processes for triaging security events;

8.3. regular testing of response plans with established metrics to track and improve Security Incident management effectiveness;

8.4. annual reviews of company-wide incident response plans and policies to reflect and share current best practices across the company;

8.5. post-incident review with root cause analysis conducted for high-severity Security Incidents, focusing on systemic improvements and learning;

8.6. incident response procedures and plans embedded in critical business processes to minimize downtime and security risks;

8.7. published system availability information to aid in Security Incident handling and reporting at https://status.atlassian.com/ , and https://www.loomstatus.com/, as applicable;

8.8. the ability for Customer to report incidents, vulnerabilities, bugs, and issues, ensuring prompt attention to concerns related to system defects, availability, security, and confidentiality;

8.9. commitment to Customer notification of the Security Incident without undue delay as set forth in Atlassian's Data Processing Addendum, including the obligation to promptly assist the Customer with necessary information for compliance with Applicable Data Protection Laws.

9. Maintenance

Atlassian maintains a comprehensive set of formal policies, controls, and practices for continued effectiveness of its Cloud Products, which includes:

9.1. regular testing of BCDR Plans with quarterly evaluations, validated by external auditors;

9.2. real-time monitoring of the availability of multiple regions with performing of regular tests for infrastructure availability and reliability;

9.3. measures outlined in Section 4 (Assessment, Authorisation and Monitoring), Section 6 (Contingency Planning) and Section 18 (System and Communications Protection).

10. Media Protection

Atlassian maintains a comprehensive set of formal policies, controls, and practices to ensure the protection of media (internal and external), which includes:

10.1. using reliable third party services (e.g. Microsoft Azure or AWS) to operate the physical infrastructure for processing Customer Data as a Sub-processor;

10.2. sanitization and degaussing of used equipment by the third party cloud service providers, including hard drives with Customer Data in line with industry standards (e.g. NIST 800-88);

10.3. full disk encryption using industry standards (e.g. AES-256) employed for data drives on servers and databases storing Customer Data, Customer Materials, and on endpoint devices;

10.4. access to Customer Data and Customer Materials is strictly limited to Atlassian-owned machines configured under a mobile device management solution, following Atlassian's Zero Trust Model architecture;

10.5. internal bring your own device (BYOD) policy ensuring that access to permitted Atlassian networks and systems is only possible via secure and compliant devices;

10.6. unattended workspaces are required to have no visible confidential data, aligning with the secure workplace guidance.

11. Physical and Environmental Protection

Atlassian maintains a comprehensive set of formal policies, controls, and practices for the physical and environmental protection of Customer Data and Customer Materials, which includes:

11.1. a safe and secure working environment with controls implemented globally at Atlassian's offices;

11.2. employing badge readers, camera surveillance, and time-specific access restrictions for enhanced security;

11.3. implementing and maintaining access logs at office buildings for investigative purposes;

11.4. multiple compliance certifications and robust physical security measures, including biometric identity verification and on-premise security, implemented by third party data center providers;

11.5. controlled access points and advanced surveillance systems as well as protective measures for power and telecommunication cables, alongside with environmental control systems, implemented by third party data center providers;

11.6. positioning critical equipment in low-risk environmental areas for added safety (both by Atlassian and its third party data center providers);

11.7. precautions to protect physical infrastructure of facilities where Customer Data or Customer Materials are hosted or otherwise processed against environmental threats, both naturally occurring and man-made, such as excessive ambient temperature, fire, flood, humidity, theft, and vandalism.

12. Planning

Atlassian maintains a comprehensive set of formal policies, controls, and practices for appropriate planning of business operations, which includes:

12.1. active monitoring and documentation by legal and compliance teams on regulatory obligations;

12.2. a detailed system security plan with comprehensive documentation on system boundaries and product descriptions;

12.3. communication to internal users and customers about significant changes to key products and services;

12.4. periodic reviews and updates of the security management program.

13. Program Management

Atlassian maintains a comprehensive set of formal policies, controls, and practices for appropriate program management, which includes:

13.1. supporting the security management program at the executive level, encompassing all security-related policies and practices;

13.2. documented information security policies, including (i) defined roles, (ii) risk mitigation, and (iii) service provider security management program;

13.3. periodic risk assessments of systems processing Customer Data, with prompt reviews of Security Incidents for corrective action;

13.4. formal security controls framework aligning to standards such as SOC 2, ISO27001, and NIST 800-53;

13.5. processes for identifying and quantifying security risks, with mitigation plans approved by the Chief Trust Officer and regular tracking of implementation;

13.6. comprehensive and diverse approach to security testing to cover a wide range of potential attack vectors;

13.7. regular review, testing and updating of the information security management program and policies integral to Atlassian's business (annually, at a minimum);

13.8. an information security management program that requires security by design approach, secure development, secure engineering, and secure operations that are consistent with industry standards;

13.9. development program for security staff with regular trainings; organizational chart that delineates roles and responsibilities;

13.10. setting and review of strategic operational objectives by the executive management;

13.11. annual review of the Enterprise Risk Management (ERM) framework, including the risk management policy, risk assessments, and fraud risk assessments, by the Head of Risk and Compliance.

14. Personnel Security

Atlassian maintains a comprehensive set of formal policies, controls and practices for the security of all Atlassian's employees who have access to Customer Data and Customer Materials, which includes:

14.1. pre-hire background checks, including criminal record inquiries, for all in-scope employees, with heightened reviews performed for senior executive and accounting roles to the extent permissible under applicable local laws;

14.2. an onboarding process that includes in-scope employees' execution of confidentiality agreements, employment contracts, and acknowledgement of applicable policies and codes of conduct;

14.3. global and local employment policies, maintained and reviewed annually;

14.4. processes for role changes and terminations including automatic de-provisioning and checklists for employee exits, with managerial approval required for re-provisioning the access;

14.5. ongoing security and compliance training for employees, with targeted training for specific roles and the presence of security champions in teams;

14.6. established disciplinary processes to manage violations of Atlassian's policies.

15. Personal Data Processing and Transparency

Atlassian maintains a comprehensive set of formal policies, controls, and practices for the compliance of personal data processing in line with Applicable Data Protection Laws, which includes:

15.1. a global privacy compliance program for reviewing and adapting to applicable data protection laws including necessary safeguards and processes;

15.2. maintaining an internal personal data processing policy with clear definitions of personal data categories, processing purposes, and processing principles;

15.3. detailed standards for processing of various categories of personal data covering the topics such as processing principles, applicable legal basis, privacy by design/by default principles, retention, and destruction;

15.4. an established method to create pseudonymised data sets using industry standard practices and appropriate technical and organisational measures governing the systems capable of remapping pseudonymous identifiers;

15.5. transparent privacy policies for its users and customers, as well as internal guidelines for employees;

15.6. comprehensive compliance documentation, including but not limited to, and where applicable, (i) a record of processing activities, (ii) privacy impact assessments, (iii) transfer impact assessments, (iv) consents, and (v) data processing agreements with customers and vendors;

15.7. secure development practices across all development lifecycle stages, focusing on security and data protection from the initial design phase;

15.8. ensuring Atlassian's compliance with data subjects' rights to access, correct, and delete their personal data in accordance with applicable data protection laws.

16. Risk Assessment

Atlassian maintains a comprehensive set of formal policies, controls, and practices for a robust Information Security Management System, which includes:

16.1. a comprehensive risk management program for identifying, assessing, and addressing various risks to support informed risk management decisions;

16.2. a policy program aligning company-wide policies with ISO 27001 and other relevant standards to mitigate associated risks;

16.3. continuous security testing and vulnerability identification, including (i) penetration tests, (ii) bug bounties, and (iii) proactive threat mitigation;

16.4. processes and metrics for reporting vulnerability management activities;

16.5. thorough security evaluations, including independent external and internal audits.

17. System and Services Acquisition

Atlassian maintains a structured, security-centric methodology for the system development, maintenance, and change management, which includes:

17.1. an agile secure software development life cycle, including the review and documentation of system and infrastructure changes;

17.2. secure, standardized application deployment with automated processes for system configuration changes and deployment;

17.3. defined development process with peer-reviewed pull requests and mandatory automated tests prior to merging;

17.4. segregated responsibilities for change management among designated employees;

17.5. emergency change processes, including "break glass" procedures, ensuring readiness for rapid response during critical incidents;

17.6. robust compliance settings in Atlassian's source code and deployment systems preventing unauthorized alterations;

17.7. clear documentation and monitoring of all configuration changes, with automatic alerts for non-compliance or alterations in peer review enforcement;

17.8. supporting documentation for Cloud and Software Products including instructions on how to securely use and configure them;

17.9. strict controls over modifications to vendor software;

17.10. regular scanning and updates of third-party or open-source libraries as well as ongoing scanning of the code base.

18. System and Communications Protection

Atlassian maintains a comprehensive set of formal policies, controls, and practices for system and communication protection which includes:

18.1. cryptographic mechanisms to safeguard sensitive information stored and transmitted over networks, including public internet, using reliable and secure encryption technologies;

18.2. encryption of Customer Data at rest using AES-256 and in transit using Transport Layer Security (TLS) 1.2+ with Perfect Forward Secrecy (PFS) across public networks;

18.3. zone restrictions and environment separation limiting connectivity between production and non-production environments;

18.4. continuous management of workstation assets including (i) security patch deployment, (ii) password protection, (iii) screen locks, and (iv) drive encryption through asset management software;

18.5. restricting access to only known and compliant devices enrolled in the MDM platform, adhering to the principles of Zero Trust Model architecture;

18.6. maintaining firewalls at corporate edges for both platform and non-platform hosted devices for additional layers of security;

18.7. maintaining network and host defense, including operating system hardening, network segmentation, and data loss prevention technologies;

18.8. established measures to ensure Customer Data and Customer Materials are kept logically segregated from other customers' data.

19. System and Information Integrity

Atlassian maintains formally established policies and practices that include the following controls and safeguards relevant for system and information integrity, in particular:

19.1. adherence to stringent data disposal protocols in line with applicable laws, reasonably ensuring that data from storage media is irrecoverable post-sanitization;

19.2. strict policies to prevent the use of production data in non-production environments, ensuring the data integrity and segregation;

19.3. centrally managed, read-only system logs; monitoring for Security Incidents; retention policies aligned with security best practices;

19.4. generating and retaining logs that record access by Atlassian personnel to Customer Data or Customer Materials with respect to systems used in providing the Products, and protection of such logs against unauthorized access, modification, and accidental or deliberate destruction;

19.5. managing endpoint compatibility with systems and applications, enhancing network security and reliability;

19.6. deploying anti-malware strategies on the relevant infrastructure and Atlassian devices for robust protection against malware threats with regular updates to malware protection policies and detection tools;

19.7. unique identifiers and token-based access control to ensure logical isolation of, and secure, limited access to, Customer Data;

19.8. segregation of production and non-production environments;

19.9. protection of Customer Data within a sandbox environment (for example, to reproduce an error) utilising similar measures to those in the production environment.

20. Supply Chain Risk Management

Atlassian maintains formally established policies and practices for supply chain risk management, which includes:

20.1. a formal framework for managing vendor relationships, and aligning the security, availability, and confidentiality standards of suppliers throughout their lifecycles;

20.2. a robust third party risk management (TPRM) assessment process including risk assessments, due diligence, contract management, and ongoing monitoring of all third parties;

20.3. dedicated teams, including legal, procurement, security, and risk departments for the review of contracts, service level agreements, and security measures to manage risks related to security and data confidentiality;

20.4. functional risk assessments of suppliers before onboarding and periodically, based on risk levels, with revisions during policy renewals or significant relationship changes;

20.5. an inventory of all suppliers detailing ownership and risk levels associated with the services provided to Atlassian;

20.6. annual review of audit reports (e.g. SOC 2) and regular reviews of information technology governance policies and security assessments of supply chain providers to ensure applicable controls are compliant;

20.7. measures to secure third-party endpoints, focusing on compliance monitoring and selective restrictions.

ANHANG IV – LISTE DER UNTERAUFTRAGSVERARBEITER (Stand: 27.10.2025)

Der Auftragsverarbeiter setzt die folgenden Unterauftragsverarbeiter ein:

Name	**Anschrift**	**Kontakt für Datenschutzfragen**	**Beschreibung der Verarbeitung**	**Mechanismus für Drittlandstransfer**
Amazon Web Services EMEA SARL	38 avenue John F. Kennedy, L-1855, Luxemburg	AWS-EU-Privacy@amazon.com	AWS Webhosting-Services (Bereitstellung und Betreuung der technischen Infrastruktur für die atmio-Software)	Im Rahmen der Einschaltung von weiteren Unterauftragsverarbeitern: Standardvertragsklauseln / für EU-US-Transfers: Angemessenheitsbeschluss (EU-US Data Privacy Framework)

Atlassian Pty Ltd	c/o Atlassian, Inc. 350 Bush Street, Floor 13 San Francisco, CA 94104	privacy@atlassian.com	JIRA Webhosting-Services (Bereitstellung und Betreuung der technischen Infrastruktur für das Ticket- und Supportsystem von atmio)	Standardvertrags-klauseln / für EU-US-Transfers: Angemessenheits-beschluss (EU-US Data Privacy Framework)