STANDARDVERTRAGSKLAUSELN

Zur Auftragsverarbeitung nach Art. 28 DSGVO

Name der verantwortlichen Organisation:	
Adresse:	
Tel.:	
Fax:	
E-Mail:	

(**Verantwortlicher**)

Und

Name der auftragsverarbeitenden Organisation:	Matrix 42 Helvetia AG
Adresse:	Sonnmatthof 3, CH-6023 Rothenburg (LU)
Tel.:	+41 41 720 42 20
Fax:	
E-Mail:	info@matrix42.com

(**Auftragsverarbeiter**)

jeweils eine "Partei"; gemeinsam "die Parteien",

HABEN die folgenden Standarddatenschutzklauseln (die Klauseln) VEREINBART, um angemessene Garantien in Bezug auf den Schutz der Privatsphäre und der Grundrechte und Grundfreiheiten natürlicher Personen für die Verarbeitung der in Anhang II genannten personenbezogenen Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen sicher zu stellen.

STANDARDVERTRAGSKLAUSELN NACH ART. 28 DSGVO

ABSCHNITT I

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 (Datenschutz-Grundverordnung) 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 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 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 erfüllt werden.

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.

3. Auslegung

a) Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 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 auszulegen.

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

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.

5. Kopplungsklausel

- Nicht anwendbar -

ABSCHNITT II - PFLICHTEN DER PARTEIEN

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.

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 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 personenbe-

zogener 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 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) ALLGEMEINE SCHRIFTLICHE GENEHMIGUNG: 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 60 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 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 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.

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 Perso-

nen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Klauseln 8.1 und 8.2 befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.

c) Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 8.2 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.

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 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:

1) 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);

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

3) 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

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 – 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 Klausel 10.1 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 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 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(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.

Unterschriften

Diese Standarddatenschutzklauseln können mittels einer elektronischen Signatur oder eines vergleichbaren elektronischen Verfahrens im Sinne von Artikel 26 der eIDAS-Verordnung (EU) Nr. 910/2014 vom 23. Juli 2014 ausgeführt werden.

Die Vertragsparteien kommen überein, dass die elektronische Signatur hinsichtlich ihrer Rechtswirkung und ihrer Zulässigkeit als Beweismittel in Gerichtsverfahren nicht wegen ihrer elektronischen Form oder ihres Fehlens für qualifizierte elektronische Signaturen verneint werden darf.

Name:

Position:

Datum:

für

Unterschrift:

Name:

Position:

Datum:

für

Unterschrift:

Name:	Unterschrift:
Position:	
Datum:	
für Matrix42 GmbH	

ANHANG I – Nicht anwendbar

ANHANG II - Beschreibung der Verarbeitung

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden:
Beschäftigte / Mitarbeiter

Kategorien personenbezogener Daten, die verarbeitet werden:
☒ Vorname ☒ Nachname ☒ Benutzername ☒ postalische berufliche Adresse ☒ Email-Adresse ☒ Telefonnummern ☒ Abteilungszugehörigkeit ☒ Berufsbezeichnung ☒ Berechtigung zur Nutzung des Supports ☒ Operative Daten im Rahmen der Nutzung der SaaS Systeme

Verarbeitete sensibler 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:
Nicht zutreffend.

Art der Verarbeitung: *Beschreibung der Verarbeitung. Was wird gemacht oderkonkreter Verweis auf den zugrunde liegenden Vertrag (z.B. Leistungs- oder Servicevertrag) in welchem eine ausreichende Beschreibung vorhanden ist.*
☒ Anlage und Pflege von personenbezogenen Daten im lokalen Supportsystem von Matrix42 zur Kommunikation mit dem Kunden im Supportfall. ☒ Information der Kunden über Produktwartungen ☒ Information der Kunden über Produkterweiterungen ☒ Anlage und Pflege von personenbezogenen Daten in den von Matrix42 zur Bereitstellung des Services genutzten Cloudsystemen. ☒ Verarbeitung personenbezogener Daten zur Verbesserung der vom Auftragsverarbeiter entwickelten Produkte durch den Einsatz künstlicher Intelligenz und statistischer Analysen.

Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden: *Detaillierte Beschreibung der Zweckes und des Gegenstands der Verarbeitung. Was wird gemacht und wie werden dafür personenbezogenen Daten konkret durch den Auftragnehmer verarbeitet ODER Verweis auf den zugrundeliegenden Vertrag (z.B. Leistungs-*

oder Servicevertrag) in welchem eine ausreichend konkrete Beschreibung vorhanden ist.
☒ Wartung und Support ☒ Implementierung ☒ Betrieb in einer Cloud für von Matrix42 vertriebenen Software ☒ Verbesserung der Produkte des Auftragsverarbeiters

Dauer der Verarbeitung:
Die Verarbeitung erfolgt für die Dauer des Hauptvertrages zur Wartung von Matrix42 Software, ☐ der zwischen dem Verantwortlichen und einem Handelspartner des Verarbeiters geschlossen wurde. ☒ der zwischen dem Verantwortlichen und dem Verarbeiter geschlossen wurde.

Bei der Verarbeitung durch (Unter-)Auftragsverarbeiter sind **auch / ebenfalls** Gegenstand, Art und Dauer der Verarbeitung anzugeben.

ANHANG III - Technische und organisatorische Maßnahmen, einschließlich zur Gewährleistung der Sicherheit der Daten

(a) Maßnahmen der Pseudonymisierung und Verschlüsselung personenbezogener Daten:

Ein administrativer Zugriff auf Serversysteme erfolgt grundsätzlich über verschlüsselte Verbindungen.

Darüber hinaus werden Daten auf Server- und Clientsystemen auf gemäß Stand der Technik verschlüsselten Datenträgern gespeichert. Es befinden sich entsprechende Festplattenverschlüsselungssysteme im Einsatz, wie z.B. BitLocker.

1) Maßnahmen zur fortdauernden Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung:

Zutrittskontrollen:

- Büroräume: Zutrittskontrolle des Gebäudes Tag/Nacht
  - Chip mit PIN
  - Schlüssel
  - Empfang
- Verschlossene Türen bei Abwesenheit
- Festlegung von Sicherheitsbereichen entsprechend Schutzbedarf
- Protokollierung der Zu- und Abgänge
- Gebäudeüberwachung durch Videoüberwachung

Zugangskontrollen:

- Der Zugangssteuerung erfolgt über Active Directory verwaltete Benutzerkonten
  - Implementierung einer Passwortrichtlinie
  - Automatische Bildschirmsperre
  - Einsatz von MFA bei erhöhtem Schutzbedarf
- Zugriffsprotokollierung
- Verschlüsselung von drahtlosen Netzwerken
- Vergabe von Zugriffsberechtigungen gem. „Need-to-Know" Prinzip
- Alle Netzwerksegmente sind mit Firewalls und entsprechenden Regeln abgesichert.

Zugriffskontrollen:

- Berechtigungskonzept
- Prozess zur Änderung / Entzug von Berechtigungen (Abteilungswechsel, Austritt)
- Verfahren zum Umgang und Einschränkung von privilegierten Berechtigungen (Administratorrechten)
- Benutzerkennung via Username und Passwort + ggf. weiteren Faktoren
- Vernichtung von Datenträgern und Dokumenten in gesicherten Containern mit Nachweis

Trennungskontrollen:

- Verpflichtung von Beschäftigten auf das Datengeheimnis
- Daten werden durch Zugriffsregelung und/oder Mandantenkonzepte oder fallweise zusätzlich durch unterschiedliche Server-Hardware (ggf. virtuell) von anderen Daten getrennt.
- Trennung von Entwicklungs-, Test- und Produktivsystem
- Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System.

Weitergabekontrollen:

- Beschäftigte sowie eingesetzte Dienstleister, bei denen ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann, sind auf das Datengeheimnis verpflichtet.
- Der Fernzugriff auf DV-Systeme ist nur über gesicherte / verschlüsselte Kommunikationsverbindungen (https und TLS) nach Stand der Technik möglich.
- Einrichtungen von Standleitungen bzw. VPN-Tunneln
- Netzwerkseparierung
- Dokumentation von Schnittstellen
- Verfahren zur sicheren Löschung von Daten
- Durchführung von Lieferantenaudits entsprechend Schutzbedarf

Eingabekontrollen:

- Eingaben im und Veränderungen an Systemen werden mittels Logfiles aufgezeichnet und überwacht
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- Protokollierung Dateizugriff durch Dokumentation der Dateiänderungen
- Protokollierung Datenbankzugriff durch Kontrolle der Protokolle

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

- Daten auf Serversystemen werden mindestens täglich inkrementell und wöchentlich vollständig gesichert. Die Sicherungsmedien werden verschlüsselt an einen physisch getrennten Ort verlegt.
- Die IT-Systeme verfügen über eine unterbrechungsfreie Stromversorgung. Im Serverraum befindet sich eine Brandmeldeanlage. Alle Serversysteme unterliegen einem Monitoring, das im Falle von Störungen unverzüglich Meldungen an einen Administrator auslöst.
- Es existiert ein Notfallplan inklusive Wiederanlaufplan.

3) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen:

- Es wird halbjährlich ein internes Audit über alle datenschutzrelevanten Maßnahmen durchgeführt.
- Alle Mitarbeiter sind zur Wahrung der Vertraulichkeit und zur Beachtung des Datenschutzes sowie Meldungen bei Vorfällen verpflichtet.
- Ein Verzeichnis von Verarbeitungstätigkeiten wird im Datenschutzmanagementsystem gepflegt und quartalsweise auf Aktualität geprüft.
- Jährliches ISO 27001 ISMS-Audit
- Durchführung interner/externer Audits im Rahmen des ISMS-Betriebes, wie z.B. Security Awareness Tests

4) Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung:

Die Sicherheit der Verarbeitung wird durch Kontrollen im Rahmen unseres ISO 27001 konformen ISMS gewährleistet. Dieses wird jährlich extern auditiert.

5) Maßnahmen zur Identifizierung und Autorisierung der Nutzer:

Wir haben angemessene Berechtigungskonzepte sowie Prozesse für Joiner/Leaver/Changer im Rahmen unseres ISO 27001 konformen ISMS umgesetzt. Dieses wird jährlich extern auditiert.

6) Maßnahmen zum Schutz der Daten während der Übermittlung:

Wir haben angemessene Berechtigungskonzepte sowie Verschlüsselungstechniken gem. Stand der Technik im Rahmen unseres ISO 27001 konformen ISMS umgesetzt. Dieses wird jährlich extern auditiert.

7) Maßnahmen zum Schutz der Daten während der Speicherung:

Wir haben angemessene Berechtigungskonzepte, Prozesse für Joiner/Leaver/Chan sowie Verschlüsselungstechniken gem. Stand der Technik im Rahmen unseres ISO 27001 konformen ISMS umgesetzt. Dieses wird jährlich extern auditiert.

8) Maßnahmen zur Gewährleistung der physischen Sicherheit von Orten, an denen personenbezogene Daten verarbeitet werden:

Wir haben angemessene Konzepte zur Zutrittssicherheit im Rahmen unseres ISO 27001 konformen ISMS umgesetzt. Dieses wird jährlich extern auditiert.

9) Maßnahmen zur Gewährleistung der Protokollierung von Ereignissen:

Wir haben angemessene Kontrollen zur Gewährleistung der Protokollierung von im Rahmen unseres ISO 27001 konformen ISMS umgesetzt. Dieses wird jährlich extern auditiert.

10) Maßnahmen zur Gewährleistung der Systemkonfiguration, einschließlich der Standardkonfiguration:

Wir haben angemessene Kontrollen zur Gewährleistung von angemessenen Systemkonfigurationen inkl. Standardkonfiguration wie z.B. Privacy by default/by design im Rahmen unseres ISO 27001 konformen ISMS umgesetzt. Dieses wird jährlich extern auditiert.

11) Maßnahmen für die interne Governance und Verwaltung der IT und der IT-Sicherheit:

IT- sowie Information Security Governance inclusive entsprechender Rollen und Prozesse wie z.B. ein benannter CISO haben wir im Rahmen unseres ISO 27001 konformen ISMS umgesetzt. Dieses wird jährlich extern auditiert.

12) Maßnahmen zur Zertifizierung/Qualitätssicherung von Prozessen und Produkten:

Betrieb eines ISMS nach ISO 27001.

13) Maßnahmen zur Gewährleistung der Datenminimierung:

- Verzeichnis von Verarbeitungstätigkeiten wird im Datenschutzmanagementsystem gepflegt und quartalsweise auf Aktualität geprüft.
- Privacy by default Systemkonfiguration

14) Maßnahmen zur Gewährleistung der Datenqualität:

- Bei Matrix42 wird halbjährlich ein internes Audit über alle datenschutzrelevanten Maßnahmen durchgeführt.

15) Maßnahmen zur Gewährleistung einer begrenzten Vorratsdatenspeicherung:

- Im Verzeichnis von Verarbeitungstätigkeiten werden die Löschanforderungen dokumentiert.
- Die Löschanforderungen werden mittels automatischer Löschverfahren bzw. manuellen Löschprozessen regelmäßig bzw. anlassbezogen innerhalb angemessener Fristen umgesetzt.

ANHANG IV - Liste der Unterauftragsverarbeiter

Erläuterung:

Dieser Anhang muss im Falle einer gesonderten Genehmigung von Unterauftragsverarbeitern ausgefüllt werden (Klausel 7.7(a), Option 1).

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

Nr.	Name:	Anschrift:	Name, Funktion und Kontaktdaten der Kontaktperson:	Beschreibung der Verarbeitung (einschließlich einer klaren Abgrenzung der Verantwortlichkeiten, falls mehrere Unterauftragsverarbeiter genehmigt werden):
1.	Matrix42 Austria GmbH	Handelskai 92 1200 Wien Österreich	Boris Samsel, VP Sales Support, boris.samsel@matrix42.com	Erweiterter Support für Remote Control (3rd level)
2.	Matrix42 Ukraine LLC	Velyka Vasylkivska St 77A Kyiv 03150 Ukraine	Anastasiia Zhytnyk, Geschäftsführerin, anastasia.kyslenko@matrix42.com	Erweiterter Support für ESM und UEM (3rd level)
3.	Matrix42 Software Engineering Romania S.R.L.	313 - 315 Barbu Vacarescu Street, 5th floor, office A-7.17. District 2, Bucharest Romania	Reinhard Knatz, Director Customer Support, Reinhard.knatz@matrix42.com	Erweiterter Support für alle Matrix42 Produkte (2nd und 3rd level)
4.	Efecte Oyj	Säterinkatu 6 02600 Espoo Finland	Sanne Asti, VP Customer Support, Sanne.Asti@matrix42.com	Erweiterter Support für alle Matrix42 Produkte (2nd und 3rd level)
5.	Neam IT-Services GmbH	Technologiepark 8 33100 Paderborn Deutschland		Premium Support - Monitoring
6.	CDS Call Dispatch Scholz GmbH	Mombacher Str. 76 55122 Mainz Deutschland		Premium Support - Call Center
7.	Telekom Deutschland GmbH	Landgrabenweg 151, 53227 Bonn		Hosting (einschließlich Beta-/Produktionsnutzung von KI-Funktionalitäten, falls zutreffend) *

* Der für die Verarbeitung Verantwortliche erklärt sich damit einverstanden, dass die Bestimmungen der Online-Service-Bedingungen (https://www.microsoft.com/de-de/licensing/product-licensing/products.aspx?rtc=1) von Microsoft und die Bestimmungen des

AVV's (https://aka.ms/DPA) von Microsoft auf die Nutzung der oben genannten Dienste Anwendung finden.