Vertrag über die Verarbeitung personenbezogener Daten im Auftrag gemäß Art. 28 DSGVO (AVV)

zwischen

Auftraggeber

und der

Ingenious Technologies AG, Friedrichstraße 171, D-10117 Berlin

- nachstehend **Auftragnehmer** genannt –

- gemeinsam auch **die Parteien** genannt –

§ 1 Vertragsgegenstand

(1) Der Auftragnehmer erbringt für den Auftraggeber Leistungen auf Grundlage des zwischen den Parteien geschlossenen Hauptvertrages. Dabei verarbeitet der Auftragnehmer personenbezogene Daten i.S.d. Art. 4 Nr. 4 DSGVO für den Auftraggeber (nachfolgend „Auftraggeber-Daten“ genannt) ausschließlich im Auftrag und nach Weisung des Auftraggebers. Rahmen und Umfang der Datenverarbeitung ergeben sich aus dem Hauptvertrag.

(2) Dem Auftraggeber obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung. Den Auftragnehmer trifft keinerlei Verpflichtung, Weisungen des Auftraggebers (datenschutz-) rechtlich zu prüfen. Ist der Auftragnehmer jedoch der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, wird er den Auftraggeber darauf hinweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis die Weisung bestätigt oder geändert wird. Räumt der Auftraggeber auf die Information über eine nach Ansicht des Auftragnehmers rechtswidrige Weisung die Bedenken des Auftragnehmers nicht aus, kann dieser die Durchführung der betreffenden Weisung ablehnen, soweit sie seine Verantwortungssphäre betrifft.

(3) Dieser Vertrag nimmt Bezug auf die folgenden durch den Auftragnehmer ausgeführten Tätigkeiten, deren konkrete Art und Umfang sich aus den jeweils geschlossenen Hauptverträgen ergibt:

- Verwaltung des exklusiven Ingenious Partnership Network und Vermittlung zwischen Advertisern und dem Auftraggeber,
- Betrieb der Ingenious SaaS-Plattform, um diese dem Auftraggeber und weiteren Kunden über das Internet zur Verfügung zu stellen,
- Durchführung von Unterstützungsleistungen und Wartungstätigkeiten für die Plattform.

(4) Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang des Auftragnehmers mit den Auftraggeber-Daten in Erfüllung des Hauptvertrages.

§ 2 Dauer der Verarbeitung

(1) Laufzeit und Kündigung dieses Vertrags richten sich nach den Bestimmungen zu Laufzeit und Kündigung des Hauptvertrags. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieses Vertrages.

(2) Eine isolierte Kündigung dieses Vertrages ist ausgeschlossen.

§ 3 Umfang, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten, Kategorien betroffener Personen

(1) Der Auftragnehmer verarbeitet die Auftraggeber-Daten ausschließlich im Auftrag und nach dokumentierter Weisung des Auftraggebers. Der Auftraggeber bleibt Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO.

(2) Die Verarbeitung der Auftraggeber-Daten im Rahmen der Auftragsverarbeitung erfolgt entsprechend der in **Anlage 1** zu diesem Vertrag enthaltenen Festlegungen zu Art und Zweck der Datenverarbeitung. Sie bezieht sich auf die in **Anlage 1** festgelegte Art der Auftraggeber-Daten und die dort aufgeführten Kategorien betroffener Personen.

(3) Die Verarbeitung der Auftraggeber-Daten findet im Gebiet der Bundesrepublik Deutschland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

§ 4 Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Verarbeitung sowie für die Wahrung der Rechte der betroffenen Personen aus den Art. 12 bis 22 DSGVO ist der Auftraggeber allein verantwortlich.

(2) Die Verarbeitung der Auftraggeber-Daten durch den Auftragnehmer im Rahmen dieser Vereinbarung erfolgt ausschließlich nach Weisung des Auftraggebers gemäß Art. 28 Abs. 3 S. 2 lit. a DSGVO, es sei denn, der Auftragnehmer ist nach dem Recht der Europäischen Union oder dem Recht des Mitgliedstaates, dem er unterliegt, zur weiteren Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(3) Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art und Zwecke der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann.

(4) Einzelweisungen nach Abschluss des Vertrages bedürfen der Textform und sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren.

(5) Erteilt der Auftraggeber Einzelweisungen hinsichtlich des Umgangs mit Auftraggeber-Daten, die über den im Hauptvertrag vereinbarten Leistungsumfang hinausgehen sind die dadurch begründeten Kosten vom Auftraggeber zu tragen.

(6) Der Auftraggeber informiert den Auftragnehmer unverzüglich und vollständig, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung von Auftraggeber-Daten durch den Auftragnehmer oder seiner Weisungen feststellt.

Weisungsempfänger beim Auftragsverarbeiter ist:

Der / die Datenschutzbeauftragte der Ingenious Technologies AG, Friedrichstraße 171, D-10117 Berlin; privacy@i19s.com

(7) Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen.

§ 5 Pflichten des Auftragnehmers

(1) Der Auftragnehmer stellt sicher, dass die Verarbeitung der Auftraggeber-Daten im Rahmen der Leistungserbringung nach dem Hauptvertrag in seinem Verantwortungsbereich, der die Unterauftragnehmer nach § 9 dieses Vertrags einschließt, in Übereinstimmung mit den Bestimmungen dieses Vertrages erfolgt.

(2) Der Auftragnehmer ist verpflichtet, dem Auftraggeber auf Antrag die erforderlichen Informationen, einschließlich Zertifizierungen sowie Überprüfungs- und Inspektionsergebnisse, die dem Nachweis der Einhaltung der in diesem Vertrag niedergelegten Pflichten dienen, zur Verfügung zu stellen.

(3) Der Auftragnehmer hat die zur Verarbeitung von Auftraggeber-Daten befugten Personen gemäß Art. 28 Abs. 3 lit. b DSGVO schriftlich zur Vertraulichkeit zu verpflichten, sofern diese nicht bereits einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(4) Der Auftragnehmer ist verpflichtet, einen fachkundigen und zuverlässigen Datenschutzbeauftragten schriftlich zu bestellen, der seine Tätigkeit gemäß der Art. 37, 38 und 39 DSGVO ausüben kann, sofern und solange die gesetzlichen Voraussetzungen für eine Bestellpflicht gegeben sind. Der Auftragnehmer wird die aktuellen Kontaktdaten des Datenschutzbeauftragten auf seiner Webseite leicht zugänglich hinterlegen (Art. 37 Abs. 7 DSGVO).

(5) Der Auftragnehmer und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DSGVO enthält. Diese Pflicht besteht nicht, wenn die Voraussetzungen von Art. 30 Abs. 5 DSGVO erfüllt sind.

(6) Der Auftragnehmer darf ohne vorherige Zustimmung durch den Auftraggeber im Rahmen der Auftragsverarbeitung keine Kopien oder Duplikate der Auftraggeber-Daten anfertigen. Hiervon ausgenommen sind jedoch Kopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung und zur ordnungsgemäßen Erbringung der Leistungen gemäß dem Hauptvertrag (einschließlich der Datensicherung) erforderlich sind, sowie Kopien, die zur Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(7) Der Auftragnehmer ist verpflichtet den Auftraggeber, im Rahmen des Zumutbaren und Erforderlichen sowie gegen Erstattung der dem Auftragnehmer hierdurch entstehenden Aufwände und Kosten, bei der Erfüllung von dessen Pflichten aus Art. 12 bis 22 sowie Art. 32 bis 36 DSGVO zu unterstützen. Die Unterstützung erfolgt unter Berücksichtigung der Art der Verarbeitung und der dem Auftragnehmer zur Verfügung stehenden Informationen sowie nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen, insbesondere bei der Beantwortung von Anträgen auf Wahrnehmung der entsprechend in Art. 12 bis 22 DSGVO genannten Rechte der betroffenen Personen (§ 10).

§ 6 **Technische und organisatorische Maßnahmen**

(1) Der Auftragnehmer trifft die erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DSGVO, insbesondere die in **Anlage 2** aufgeführten Maßnahmen der Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle und Trennungskontrolle.

(2) Da die technischen und organisatorischen Maßnahmen dem technischen Fortschritt und der technologischen Weiterentwicklung unterliegen, ist es dem Auftragnehmer gestattet, alternative und adäquate Maßnahmen umzusetzen, sofern dabei das Sicherheitsniveau der in **Anlage 2** festgelegten Maßnahmen nicht unterschritten wird. Der Auftragnehmer wird solche Änderungen dokumentieren. Wesentliche Änderungen der Maßnahmen bedürfen der vorherigen Zustimmung des Auftraggebers.

§ 7 Mitzuteilende Verstöße des Auftragnehmers

(1) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er feststellt, dass er oder ein Mitarbeiter bei der Verarbeitung von Auftraggeber-Daten gegen datenschutzrechtliche Vorschriften oder gegen Festlegungen aus diesem Vertrag verstoßen haben, sofern die Gefahr einer Verletzung des Schutzes personenbezogener Daten des Auftraggebers im Sinne des Art. 4 Nr. 12 DSGVO besteht.

(2) Soweit den Auftraggeber aufgrund eines Vorkommnisses nach Absatz (1) gesetzliche Informationspflichten wegen einer unrechtmäßigen Kenntniserlangung von Auftraggeber-Daten (insbesondere nach Art. 33 und 34 DSGVO) treffen, hat der Auftragnehmer den Auftraggeber bei der Erfüllung der Informationspflichten auf dessen Ersuchen im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden Aufwände und Kosten zu unterstützen.

(3) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen, informiert hierüber den Auftraggeber und ersucht um weitere Weisungen.

(4) Meldungen nach Art. 33 oder 34 DSGVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung des Auftraggebers durchführen.

§ 8 Kontrollrechte des Auftragsgebers

(1) Der Auftraggeber überzeugt sich auf eigene Kosten vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers gemäß **Anlage 2** und dokumentiert das Ergebnis. Dies geschieht durch Einholung einer Selbstauskunft des Auftragnehmers, die dieser auch durch Vorlage eines geeigneten Zertifikats eines Sachverständigen erfüllen kann.

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf schriftliche Anforderung alle erforderlichen Auskünfte und Informationen bezüglich seiner Pflichten aus dieser Vereinbarung zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen der **Anlage 2** nachzuweisen. Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 oder Zertifizierungen nach gemäß Art. 42 DSGVO; aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren); eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz), erfolgen.

(3) Der Auftraggeber oder ein entsprechend Beauftragter haben das Recht vorgenannte Kontrollen zu den üblichen Geschäftszeiten vorzunehmen. Diese Kontrollen sind rechtzeitig (in der Regel mindestens zwei Wochen vorher) anzukündigen und haben den Betriebsablauf beim Auftragnehmer so wenig wie möglich zu beeinträchtigen.

(4) Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Kontrolle, hat der Auftraggeber den Dritten schriftlich ebenso zu verpflichten, wie auch der Auftraggeber aus diesem Vertrag verpflichtet ist. Zudem hat er den Dritten auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen des Auftragnehmers hat der Auftraggeber diesem die Verpflichtungsvereinbarungen mit dem Dritten vorzulegen. Der Auftraggeber darf keinen Wettbewerber des Auftragnehmers mit der Kontrolle beauftragen.

§ 9 **Unterauftragsverhältnisse**

(1) Der Auftraggeber stimmt der Beauftragung der in **Anlage 3** aufgeführten Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 1 bis 4 DSGVO ausdrücklich zu. Dem Auftragnehmer ist die Beauftragung weiterer Unterauftragnehmer (weitere Auftragsverarbeiter) gestattet.

(2) Der Auftragnehmer wird den Auftraggeber unverzüglich über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Unterauftragnehmer informieren. Gegen derartige Änderungen darf der Auftraggeber aus wichtigem, dem Auftragnehmer nachzuweisenden Grund, Einspruch erheben. Der Einspruch ist binnen einer Frist von einer Woche ab Zugang einer entsprechenden Mitteilung des Auftragnehmers schriftlich auszusprechen.

(3) Keiner Mitteilung bedarf die Einschaltung von Unterauftragnehmern, bei denen der Unterauftragnehmer lediglich eine Nebenleistung zur Unterstützung bei der Leistungserbringung nach dem Hauptvertrag in Anspruch nimmt, z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder zur Entsorgung von Datenträgern sowie für sonstige Maßnahmen

(4) zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen, auch wenn dabei ein Zugriff auf Auftraggeber-Daten nicht ausgeschlossen werden kann. Der Auftragnehmer wird auch diese mit der gebotenen Sorgfalt auswählen und im erforderlichen Umfang Vereinbarungen treffen, um einen angemessenen Schutz der Auftraggeber Daten zu gewährleisten.

(5) Im Fall der Hinzuziehung eines Unterauftragnehmers erlegt der Auftragnehmer diesem, im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats, dieselben Datenschutzpflichten auf, die in diesem Vertrag festgelegt sind. Der Vertrag ist so auszugestalten, dass es dem Auftraggeber möglich ist, im Bedarfsfall angemessene Überprüfungen und Inspektionen beim Unterauftragnehmer, auch vor Ort durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

(6) Sofern eine Einbeziehung von Unterauftragnehmern in einem Drittstaat erfolgen soll, stellt der Auftragnehmer sicher, dass beim Unterauftragnehmer ein entsprechendes Datenschutzniveau gewährleistet ist (z.B. durch Abschluss einer Vereinbarung auf Basis von EU-Standarddatenschutzklauseln).

(7) Auf Verlangen wird der Auftragnehmer dem Auftraggeber den Abschluss der vorgenannten Vereinbarungen mit seinen Unterauftragnehmern nachweisen.

§ 10 Rechte der betroffenen Personen

(1) Die Rechte der durch die Datenverarbeitung betroffenen Personen sind gegenüber dem Auftraggeber geltend zu machen.

(2) Soweit eine betroffene Person sich unmittelbar an den Auftragnehmer zur Wahrnehmung ihrer Rechte gemäß der Art. 12 bis 22 DSGVO der sie betreffenden Daten wenden sollte, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen.

(3) Im Übrigen gilt § 5 Abs. (7) dieser Vereinbarung.

§ 11 Haftung

(1) Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haften Auftraggeber und Auftragnehmer als Gesamtschuldner.

(2) Für den Ersatz von Schäden, die eine betroffene Person wegen einer nach dem geltenden Datenschutzrecht unzulässigen oder unrichtigen Verarbeitung von

(3) Auftraggeber-Daten im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zum Auftragnehmer alleine der Auftraggeber verantwortlich.

(4) Der Auftraggeber verpflichtet sich, den Auftragnehmer im Innenverhältnis von allen Ansprüchen Dritter frei zu stellen, solange und soweit er nicht nachweist, dass der Auftragnehmer seinen speziell den Auftragnehmer treffenden Pflichten aus der DSGVO nicht nachgekommen ist oder unter Nichtbeachtung einer rechtmäßig erteilten Weisung des Auftraggebers oder gegen eine rechtmäßig erteilte Weisung gehandelt hat.

(5) Sollte eine Datenschutzbehörde oder ein Gericht gegen den Auftragnehmer eine Geldbuße auf Grund einer Datenverarbeitung des Auftragnehmers verhängen, die auf einer Weisung des Auftraggebers beruht, hat der Auftraggeber dem Auftragnehmer den entsprechenden Betrag auf schriftliche Mitteilung hin in voller Höhe innerhalb von 30 Tagen ab der schriftlichen Mitteilung zu erstatten.

(6) Der Auftraggeber hat dem Auftragnehmer sämtliche sich aus der von ihm zu vertretenden Rechtsverletzung gemäß Absatz 3 und 4 ergebenden Kosten zu erstatten, einschließlich der Kosten der Rechtsverfolgung.

(7) Unbeschränkte Haftung: Der Auftragnehmer haftet unbeschränkt für Vorsatz und grobe Fahrlässigkeit, bei Verletzung einer vertraglich gewährten Garantie sowie nach Maßgabe des Produkthaftungsgesetzes. Für leichte Fahrlässigkeit haftet der Auftragnehmer bei Schäden aus der Verletzung des Lebens, des Körpers und der Gesundheit von Personen. Im Übrigen gilt folgende beschränkte Haftung: Bei leichter Fahrlässigkeit haftet der Auftragnehmer nur im Falle der Verletzung einer wesentlichen Vertragspflicht des Hauptvertrages, deren Erfüllung die ordnungsgemäße Durchführung des Hauptvertrages überhaupt erst ermöglicht und auf deren Einhaltung der Auftraggeber regelmäßig vertrauen darf (Kardinalpflicht). Die Haftung für leichte Fahrlässigkeit ist der Höhe nach beschränkt auf die bei Vertragsschluss vorhersehbaren Schäden, mit deren Entstehung typischerweise gerechnet werden muss.

§ 12 Rückgabe und Löschung überlassener Auftraggeber-Daten

(1) Der Auftragnehmer hat sämtliche Auftraggeber-Daten nach Beendigung der vertragsgegenständlichen Leistungserbringung (insbesondere bei Kündigung oder sonstiger Beendigung des Hauptvertrags), nach Wahl des Auftraggebers, zurückzugeben oder zu löschen und bestehende Kopien zu vernichten, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der Daten besteht.

(2) Der Auftragsnehmer hat die Löschung bzw. Vernichtung von Auftraggeber-Daten zu dokumentieren und den Nachweis dem Auftraggeber auf Anforderung nachzuweisen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung oder gesetzlichen Aufbewahrungsfristen dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

§ 13 **Sonstiges**

(1) Soweit in diesem Vertrag keine Sonderregelungen enthalten sind, gelten die Bestimmungen des Hauptvertrags. Im Fall von Widersprüchen zwischen diesem Vertrag und Regelungen aus sonstigen Vereinbarungen, insbesondere aus dem Hauptvertrag, gehen die Regelungen aus diesem Vertrag vor.

(2) Der Auftraggeber und der Auftragnehmer und gegebenenfalls deren Vertreter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

Stand: 12. Mai 2026

Anlagen:

Anlage 1 Zwecke und Art der Datenverarbeitung, Art der Daten und Kategorien betroffener Personen

Anlage 2 Technische und organisatorische Maßnahmen

Anlage 3 Zulässige Unterauftragnehmer

Anlage 1

Zweck und Art der Datenverarbeitung, Art der Daten und Kategorien der betroffenen Personen

Der Auftragnehmer erbringt die nach dieser Anlage vereinbarten Leistungen gegenüber dem Auftraggeber ausschließlich nach Weisung des Auftraggebers und auf Grundlage der zwischen den Parteien geschlossenen Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag.

Der Auftragnehmer verarbeitet im Auftrag des Auftraggebers nachfolgende personenbezogene Daten zu den genannten Zwecken:

Art der Daten	Art und Zweck der Datenverarbeitung	Kategorien der betroffenen Personen
• **Kurzname** • **Nachname** • **Titel** • **Vorname** • **Personalnummer (geschäftlich)** • **E-Mail-Adresse (geschäftlich)** • **Messenger-Adresse (geschäftlich)** • **Telefonnummer (geschäftlich)** • **Adresse (geschäftlich)**	**KYC-Prüfung, Onboarding**	**Vertretungsberechtige Person des Auftraggebers**
• **Kurzname** • **Nachname** • **Titel** • **Vorname** • **Personalnummer (geschäftlich)** • **E-Mail-Adresse (geschäftlich)** • **Messenger-Adresse (geschäftlich)** • **Telefonnummer (geschäftlich)** • **Adresse (geschäftlich)**	**Vertragspflege, Kommunikation**	**Kontaktperson des Auftraggebers**

• **Kurzname** • **Nachname** • **Titel** • **Vorname** • **Personalnummer (geschäftlich)** • **E-Mail-Adresse (geschäftlich)** • **Messenger-Adresse (geschäftlich)** • **Telefonnummer (geschäftlich)** • **Adresse (geschäftlich)** • **Positionsprofil und Funktion im Unternehmen**	**Produktfunktionalität**	**Mitarbeiter/Beschäftigte des Auftraggebers**
• **Kurzname** • **Nachname** • **Titel** • **Vorname** • **Personalnummer (geschäftlich)** • **E-Mail-Adresse (geschäftlich)** • **Messenger-Adresse (geschäftlich)** • **Telefonnummer (geschäftlich)** • **Adresse (geschäftlich)** • **Positionsprofil und Funktion im Unternehmen** • **Transaktionsdaten**	**Anonymisierung personenbezogener Daten zum Zwecke der Weiterverarbeitung aggregierter Daten, etwa für Übersichten und Zusammenfassung**	**Nutzer, Mitarbeiter/Beschäftigte des Auftraggebers**
• **Kurzname** • **Nachname** • **Titel** • **Vorname** • **Personalnummer (geschäftlich)** • **E-Mail-Adresse (geschäftlich)** • **Messenger-Adresse (geschäftlich)** • **Telefonnummer (geschäftlich)** • **Adresse (geschäftlich)** • **Positionsprofil und Funktion im Unternehmen** • **Transaktionsdaten**	**Produktfunktionalität**	**Mitarbeiter/Beschäftigte von Kunden/Partnern des Auftraggebers**

ANLAGE 2 zum Vertrag über die Verarbeitung personenbezogener Daten im Auftrag

Technische und organisatorische Maßnahmen gemäß § 64 Abs. 3 BDSG-neu

Der Auftragnehmer (AN) sichert dem Auftraggeber (AG) zu, folgende technische und organisatorische Maßnahmen gemäß § 64 Abs. 3 BDSG-neu und der dazugehörigen Anlage getroffen zu haben:

1. Zugangskontrolle

Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte.

Die Applikationsserver des AN werden ausschließlich in den Rechenzentren der jeweiligen Cloud Services Provider in dem Gebiet der Europäischen Union gehostet, so findet die Datenspeicherung und Datenverarbeitung von Personenbezogenen Daten ausschließlich in dem EU-Gebiet statt. Der physische Zugang zu den Einrichtungen, mit denen personenbezogene Daten verarbeitet wird, ist durch den jeweiligen Cloud Services Provider ausschließlich auf benannte autorisierte Personen beschränkt, so dass der Zutritt zu IT-Systemen und Datenverarbeitungsanlagen für unbefugten Personen verwehrt wird.

In der Cloud verwendet der AN sowohl Platform as a Service Dienste (PaaS) als auch Infrastructure as a Service Dienste (IaaS).

Für die Plattform as a Service (PaaS) Dienste:
Cloud Provider führt regelmäßige Systemupdates und Patches auf den unterliegenden physischen und virtuellen Maschinen durch.

Für die Infrastructure as a Service (IaaS):
Der AN führt regelmäßige OS-Aktualisierungen und Sicherheitsupdates auf allen virtuellen Maschinen des Cloud IaaS durch.

Beschreibung des Zugangskontrollsystems:

☒	Alarmanlage	☒	Absicherung von Gebäudeschächten
☒	Automatisches Zugangskontrollsystem	☒	Chipkarten-/Transponder-Schließsystem
☒	Schließsystem mit Codesperre	☒	Manuelles Schließsystem
☐	Biometrische Zugangssperren	☒	Videoüberwachung der Zugänge
☒	Lichtschranken / Bewegungsmelder	☒	Sicherheitsschlösser
☒	Schlüsselregelung (Schlüsselausgabe etc.)	☒	Personenkontrolle beim Pförtner / Empfang
☒	Protokollierung der Besucher	☒	Sorgfältige Auswahl von Reinigungspersonal
☒	Sorgfältige Auswahl von Wachpersonal	☒	Tragepflicht von Berechtigungsausweisen

2. Datenträgerkontrolle

Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern.

Die Daten werden auf logischen Datenträgern gespeichert, der physische Transport der Datenträger findet nicht statt, da die Anwendungs-Infrastruktur vollständig beim Cloud Services Provider betrieben wird. Für die Verbindung vom Office zum Rechenzentrum wird eine VPN-Verbindung verwendet (Verschlüsselung: AES 256). Die Übermittlung der personenbezogenen Daten zwischen dem Backend und dem Anwender-UI erfolgt mit einer SSL-Verschlüsselung (minimale erlaubte Verschlüsselung: TLS 1.0). Die Speicherung von nichtverschlüsselten Personenbezogenen Daten in getrennten Applikationsmodulen erfolgt in einer pseudonymisierten Form, so dass die Zuordnung der Daten zu Personen nur über die Referenz-IDs erfolgen kann. Die AN IT-Administratoren haben keinen Zugriff auf gespeicherte personenbezogene Daten, da die einzelnen Datensätze durch die Applikationslogik verschlüsselt und nur durch die Applikationslogik wieder entschlüsselt werden können.

Beschreibung der Datenträgerkontrollsystems:

☒	Verwaltung der Rechte durch Systemadministrator	☒	Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
☒	Anzahl der Administratoren auf das „Notwendigste“ reduziert	☐	Beim physischen Transport: sichere Transportbehälter/-verpackungen
☒	Erstellen eines Berechtigungskonzepts	☐	Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und -fahrzeugen
☒	Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel	☒	Verschlüsselung/Passwortschutz von Datenträgern in Laptops / Notebooks
☒	Verschlüsselung von Datenträgern	☒	Sichere Aufbewahrung von Datenträgern
☒	physische Löschung von Datenträgern vor Wiederverwendung	☒	ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)
☐	Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)	☐	Protokollierung der Vernichtung

3. Speicherkontrolle

Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten.

Die Erteilung und Änderung der Zugriffsrechte für die AN-Anwendungsadministratoren erfolgt durch die Rollen- und Rechteverwaltung in der Anwendung. Die AN IT-Administratoren haben keinen Zugriff auf gespeicherte personenbezogene Daten, da die einzelnen Datensätze durch die Applikationslogik verschlüsselt und nur durch die Applikationslogik wieder entschlüsselt werden können. Die physikalische Speicherung der Daten erfolgt in der Cloud auf die logische Storage-Einheiten, so dass die Daten dabei fragmentiert und auf mehrere physikalische Laufwerke aufgeteilt werden. Die Daten-Fragmente werden beim Lesen durch die Software-Layer erneut zusammengesetzt.

Beschreibung des Speicherkontrollsystems:

☒	Fragmentierung der Daten bei Speicherung	☒	Verschlüsselung von Datenträgern
☒	Authentifikation mit Benutzername / Passwort	☒	Verschlüsselung/Passwortschutz von Datenträgern in Laptops / Notebooks
☐	Authentifikation mit biometrischen Verfahren	☒	Zuordnung von Benutzerprofilen zu Mandanten

4. Benutzerkontrolle

Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte.

Die AN IT-Infrastruktur befindet sich vollständig in der Cloud. Die IT-Administratoren haben Zugang ausschließlich über persönliche asymmetrische RSA-Keys (2048 Bit), die Keys sind zusätzlich mit individuellen Passwörtern geschützt. Die Anmeldungen der IT-Administratoren auf den Servern werden protokolliert. Jede Erteilung bzw. Änderung der Zugriffsrechte erfolgt nach Vier-Augen-Prinzip und wird protokolliert. Die Erforderlichkeit der Zugriffsrechte der Nutzer wird regelmäßig, alle 90 Tage überprüft. Der Offboarding-Prozess stellt sicher, dass Nutzerzugänge im Falle eines Ausscheidens rechtzeitig widerrufen werden. Die Benutzerkennungen sind eindeutig und individuell. Die Passwörter sind min. 8 Zeichen lang und müssen Ziffern, Sonderzeichen sowie kleine und große Buchstaben enthalten. Die Passwörter müssen nach 90 Tagen geändert werden. In der Passwort-Historie werden die 6 letzten Passwörter gespeichert. Nach 3-facher Fehleingabe erfolgt eine automatische Account-Sperrung.

Beschreibung des Benutzerkontrollsystems:

☒	Zuordnung von Benutzerprofilen zu IT-Systemen	☒	Verwaltung der Rechte durch Systemadministrator
☒	Authentifikation mit Benutzername / Passwort	☐	Authentifikation mit biometrischen Verfahren
☒	Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel	☒	Einsatz von VPN-Technologie
☒	Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten	☒	Einsatz von Anti-Viren-Software

5. Zugriffskontrolle

Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben.

Die Überwachung des Berechtigungskonzeptes auf der Applikationsebene obliegt dem AG. Das dafür notwendige UI zum Verwalten der Rollen und der Zugriffsrechte wird vom AN zur Verfügung gestellt. Die Änderungen werden protokolliert. Die Erteilung und Änderung der Zugriffsrechte für die AN-Anwendungsadministratoren erfolgt durch dieselbe Rollen- und Rechteverwaltung in der Anwendung.

Beschreibung des Zugriffskontrollsystems:

☒ Erstellen eines Berechtigungskonzepts	☒ Verwaltung der Rechte durch Anwendungs-Administratoren
☒ Anzahl der Administratoren auf das „Notwendigste“ reduziert	☒ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
☒ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten	☒ Mandantentrennung

6. Übertragungskontrolle

Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.

Es werden keine Daten weitergegeben, da die Infrastruktur vollständig beim Cloud Provider betrieben wird. Für die Verbindung vom Office zum Rechenzentrum wird eine VPN-Verbindung verwendet (Verschlüsselung: AES 256). Die Übermittlung der personenbezogenen Daten zwischen dem Backend und dem Anwender-UI erfolgt mit einer SSL-Verschlüsselung (minimale erlaubte Verschlüsselung: TLS 1.0). Die Speicherung von nichtverschlüsselten Personenbezogenen Daten in getrennten Applikationsmodulen erfolgt in einer pseudonymisierten Form, so dass die Zuordnung der Daten zu Personen nur über die Referenz-IDs erfolgen kann.

Beschreibung der Weitergabekontrolle:

☒ Einrichtungen von Standleitungen bzw. VPN-Tunneln

☐ E-Mail-Verschlüsselung

☐ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen

☒ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form

☐ Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen

7. Eingabekontrolle

Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind.

Die Änderungen werden in derselben Datenbank protokolliert, in der auch die zu ändernden Daten gespeichert werden. So gelten für die Protokollierungsdaten die gleichen Regeln wie für die Daten selbst. Die Log-Dateien der Applikationsserver verlassen das geschützte Netzwerk nicht und werden nach 30 Tagen gelöscht. Nur die AN IT-Administratoren haben Zugriff auf das geschützte Netzwerk. Der Zugriff erfolgt über den asymmetrischen RSA-Verfahren mit der 2048-Bit Key-Länge (individuelle Keys).

Beschreibung des Eingabekontrollsystems:

☒ Protokollierung der Eingabe, Änderung und Löschung von Daten

☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

☐ Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.

☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind

8. Transportkontrolle

Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden.

Es werden keine Daten sowie Datenträger transportiert, da die Infrastruktur vollständig beim Cloud Services Provider betrieben wird. Für die Verbindung vom Office zum Rechenzentrum wird eine VPN-Verbindung verwendet (Verschlüsselung: AES 256). Die Übermittlung der personenbezogenen Daten zwischen dem Backend und dem Anwender-UI erfolgt mit einer SSL-Verschlüsselung (minimale erlaubte Verschlüsselung: TLS 1.0). Die Speicherung von nichtverschlüsselten Personenbezogenen Daten in getrennten Applikationsmodulen erfolgt in einer pseudonymisierten Form, so dass die Zuordnung der Daten zu Personen nur über die Referenz-IDs erfolgen kann.

Beschreibung der Transportkontrollsystems:

☒	Einrichtungen von Standleitungen bzw. VPN-Tunneln	☒	Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
☐	E-Mail-Verschlüsselung	☐	Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
☐	Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und -fahrzeugen	☐	Beim physischen Transport: sichere Transportbehälter/-verpackungen

9. Wiederherstellbarkeit

Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

Es werden regelmäßig Backups der Daten erstellt. Die Backups werden in demselben geschützten Netzwerk aufbewahrt, in dem auch die Daten verarbeitet werden. Die physikalische Speicherung der Backups erfolgt in der Cloud Umgebung auf den dedizierten logischen Storage-Einheiten.

Beschreibung des Wiederherstellbarkeitssystems:

☒	Unterbrechungsfreie Stromversorgung (USV)	☒	Klimaanlage in Serverräumen
☒	Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen	☒	Schutzsteckdosenleisten in Serverräumen
☒	Feuer- und Rauchmeldeanlagen	☐	Feuerlöschgeräte in Serverräumen
☒	Alarmmeldung bei unberechtigten Zutritten zu Serverräumen	☒	Erstellen eines Backup- & Recoverykonzepts
☒	Testen von Datenwiederherstellung	☒	Erstellen eines Notfallplans
☒	Aufbewahrung von Datensicherung in separaten logischen Storage-Einheiten	☒	Serverräume nicht unter sanitären Anlagen

10. Zuverlässigkeit

Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

Die IT-Infrastruktur und die Funktionsfähigkeit der Anwendung wird permanent auf mehreren Ebenen überwacht. Bei Störungen werden qualifizierte Mitarbeiter alarmiert. Die Behebung der Störungen erfolgt nach dem Notfallplan.

Beschreibung des Zuverlässigkeitssystems:

☒	Monitoring der IT-Infrastruktur und der Anwendung auf mehreren Ebenen	☒	Feuer- und Rauchmeldeanlagen
☒	Alarmierung durch E-Mails und SMS	☒	Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
☒	Erstellen eines Notfallplans	☒	Serverräume nicht unter sanitären Anlagen

11. Datenintegrität

Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.

In der Applikationslogik werden umfangreiche Regeln zum Prüfen und Sicherstellen der Datenintegrität implementiert. In der Datenbank wird Datenintegrität u.A. durch Normalisierungskonzepte und Constraints sichergestellt.

Beschreibung des Datenintegritätssystems:

- ☒ Regeln zum Verifizieren der Daten bei der Eingabe und Änderungen
- ☒ Constraints auf Datenbankobjekten
- ☒ Daten-Normalisierung

12. Auftragskontrolle

Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Die Auswahl der Unterauftragnehmer erfolgt unter größter Sorgfalt, die Verarbeitung der Daten erfolgt auf Basis des AV-Vertrages gemäß Art. 28 Datenschutz-Grundverordnung.

Beschreibung des Auftragskontrollsystems:

- ☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- ☒ vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
- ☒ schriftliche Weisungen an den Auftragnehmer (z.B. durch Datenverarbeitungsvertrag)
- ☒ Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
- ☒ Auftragnehmer hat Datenschutzbeauftragten bestellt
- ☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- ☒ Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
- ☒ laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten

13. Verfügbarkeitskontrolle

Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind.

Die Backups werden in demselben geschützten Netzwerk aufbewahrt, in dem auch die Daten verarbeitet werden. Keine Datenträger verlassen das geschützte Netzwerk. Die physikalische Speicherung der Daten erfolgt in der Cloud auf die logische Storage-Einheiten, so dass die Daten dabei fragmentiert und auf mehrere physikalische Laufwerke aufgeteilt werden. Die Daten-Fragmente werden beim Lesen durch die Software-Layer erneut zusammengesetzt. Nur die AN IT-Administratoren haben Zugriff auf das Netzwerk. Der Zugriff erfolgt über den asymmetrischen RSA-Verfahren mit der 2048-Bit Key-Länge (individuelle Keys).

Beschreibung des Verfügbarkeitskontrollsystems:

☒	Unterbrechungsfreie Stromversorgung (USV)	☒	Klimaanlage in Serverräumen
☒	Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen	☒	Schutzsteckdosenleisten in Serverräumen
☒	Feuer- und Rauchmeldeanlagen	☐	Feuerlöschgeräte in Serverräumen
☒	Alarmmeldung bei unberechtigten Zutritten zu Serverräumen	☒	Erstellen eines Backup- & Recoverykonzepts
☒	Testen von Datenwiederherstellung	☒	Erstellen eines Notfallplans
☒	Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort	☒	Serverräume nicht unter sanitären Anlagen

14. Trennbarkeit

Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können.

Bei der Speicherung der Kundendaten besteht eine logische, bei der Verarbeitung die physikalische Mandantentrennung. Produktiv- und Testsysteme sind voneinander physikalisch getrennt. Die Speicherung von nichtverschlüsselten Personenbezogenen Daten in getrennten Applikationsmodulen erfolgt in einer pseudonymisierten Form, so dass die Zuordnung der Daten zu Personen nur über die Referenz-IDs erfolgen kann.

Beschreibung des Trennbarkeitssystems:

☐	physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern	☒	Logische Mandantentrennung (softwareseitig)
☒	Erstellung eines Berechtigungskonzepts	☐	Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
☐	Versehen der Datensätze mit Zweckattributen/Datenfeldern	☐	Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System
☒	Festlegung von Datenbankrechten	☒	Trennung von Produktiv- und Testsystem

ANLAGE 3 zum Vertrag über die Verarbeitung personenbezogener Daten im Auftrag

Genehmigte Unterauftragsverarbeiter

Unterauftragsverarbeiter	Kontaktdaten
Google Ireland Ltd.	Gordon House Barrow St Dublin 4 Ireland
Atlassian Inc.	350 Bush St, Floor 13 San Francisco CA 94104 United States of America
Slack Technologies, Inc.	500 Howard Street San Francisco CA 94105 United States of America