Auftragsverarbeitungsvertrag (AVV) der CODIGO GmbH

Version 2.0 – Stand: 11.11.2026

Diese Vereinbarung zur Auftragsverarbeitung wird zwischen den Parteien als ergänzende Regelung zur Einhaltung der datenschutzrechtlichen Verpflichtungen gemäß Art. 28 der Datenschutz-Grundverordnung (DSGVO) getroffen. Sie konkretisiert die Rechte und Pflichten der Vertragsparteien im Rahmen der im Hauptvertrag beschriebenen Leistungen.

Der Partner (nachfolgend „Auftraggeber") nutzt die Leistungen der Codigo GmbH (nachfolgend „Auftragnehmer"), um seinen eigenen Kunden sowie weiteren natürlichen Personen (nachfolgend zusammenfassend „Nutzer") einen digitalen Datensafe zur Vorsorge und Nachlassverwaltung bereitzustellen.

Sofern in diesem Vertrag der Begriff „Datenverarbeitung" oder „Verarbeitung" benutzt wird, wird die Definition gemäß Art. 4 Nr. 2 DSGVO zugrunde gelegt.

§ 1 Gegenstand, Dauer und Spezifizierung

(1) Aus der Anlage 1 und dem Hauptvertrag mit dem Auftragnehmer ergeben sich Gegenstand des Auftrags, sowie Art und Zweck der Verarbeitung sowie Kategorien betroffener Daten.

(2) Die Laufzeit des Vertrages richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrecht ergeben.

(3) Ein außerordentliches Kündigungsrecht jeder Partei bleibt unberührt.

§ 2 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag und nur auf dokumentierte Weisung des Auftraggebers, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedsstaates, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor Beginn der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Dies umfasst Tätigkeiten, die im Vertrag und ggf. in einer gesonderten Leistungsbeschreibung konkretisiert sind. Der Auftraggeber und Auftragnehmer sind jeweils selbst für die Einhaltung des geltenden Datenschutzrechts verantwortlich. Der Auftraggeber bleibt für die Beurteilung der Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Beurteilung der Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DSGVO).

(2) Die Weisungen werden durch Vertrag festgelegt und können vom Auftraggeber danach schriftlich oder in Textform (z. B. E-Mail) an den vom Auftragnehmer bezeichneten Kontakt durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform vom Auftraggeber zu bestätigen.

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf personenbezogene Daten, die Gegenstand des Auftrags sind, nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DSGVO vor und dessen Voraussetzungen werden gewahrt.

(2) Der Auftragnehmer wird den Auftraggeber informieren, wenn nach seiner Auffassung eine Weisung des Auftraggebers gegen die DSGVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde. Der Auftragnehmer ist indessen nicht verpflichtet, eine umfassende rechtliche Prüfung durchzuführen. Der Auftraggeber trägt alle Mehrkosten, die dem Auftragnehmer durch eine zusätzliche oder abweichende Weisung entstehen, es sei denn, die Weisung ist erforderlich, um die geltenden gesetzlichen Anforderungen zu erfüllen.

(3) Der Auftragnehmer wird technische und organisatorische Maßnahmen (TOM) zum angemessenen Schutz der personenbezogenen Daten des Auftraggebers treffen, die den Anforderungen des Art. 32 DSGVO genügen. Der Auftragnehmer hat insbesondere TOM zu treffen, gemessen am Risiko für die Rechte und Freiheiten der betroffenen Personen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer gewährleisten. Die Vertragsparteien haben die in Anlage 2 beschriebenen TOM vereinbart. Sie sind sich darüber einig, dass die Umsetzung der beschriebenen TOM ein angemessenes Schutzniveau in Übereinstimmung mit der DSGVO gewährleistet und ausreichende Garantien zum Schutz der Rechte der betroffenen Person bietet. Die Beurteilung des angemessenen Schutzniveaus trägt dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie der für die betroffenen Personen unterschiedlichen Eintrittswahrscheinlichkeit und Schwere von Risiken gebührend Rechnung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Diese, sowie Änderungen und Ergänzungen sind vom Auftragnehmer entsprechend zu dokumentieren und dem Auftraggeber auf Anfrage zur Kenntnis zu geben. Dabei darf das Sicherheitsniveau der in Anlage 2 genannten Maßnahmen nicht unterschritten werden.

(4) Der Auftragnehmer unterstützt den Auftraggeber angesichts der Art der Verarbeitung nach Möglichkeit mit geeigneten TOM bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DSGVO, siehe hierzu die ergänzenden Regelungen im § 5.

(5) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten. Der Auftragnehmer stellt sicher, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Beschäftigten und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner stellt der Auftragnehmer sicher, dass sich die mit der Verarbeitung der personenbezogenen Daten zuständigen Personen zur Vertraulichkeit verpflichtet haben und diese Vertraulichkeitsverpflichtung auch nach Beendigung des Auftrags fortbesteht.

(6) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden in der Art und Weise, dass der Auftraggeber seinen gesetzlichen Pflichten, insbesondere nach Art. 33, 34

DSGVO, sowohl hinsichtlich des Umfangs als auch hinsichtlich der Frist nachkommen kann. Eine Meldung von Datenschutzverletzungen muss mindestens enthalten:

a. eine Beschreibung des Vorfalls, soweit möglich mit Angabe der Art der Verletzung des Schutzes personenbezogener Daten, Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der vermutlichen Zahl der betroffenen personenbezogenen Datensätze
b. Kontaktdaten einer Anlaufstelle für weitere Informationen über die Verletzung des Schutzes personenbezogener Daten
c. eine Beschreibung der voraussichtlichen Folgen des gemeldeten Vorfalls, eine Beschreibung der ergriffenen Maßnahmen oder vorgeschlagenen zur Behebung und ggf. Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen aus Sicht des Auftragnehmers

Wenn und soweit die Informationen nicht zur gleichen Zeit bereitgestellt werden können, können diese ohne unangemessene weitere Verzögerung schrittweise zur Verfügung gestellt werden

(7) Der Auftragnehmer nennt dem Auftraggeber einen verantwortlichen Kontakt für im Rahmen der Vereinbarung anfallende Datenschutzfragen.

(8) Nach Beendigung des Auftrags gibt der Auftragnehmer sämtliche Daten, Datenträger und Dokumente, soweit sie vom Auftraggeber stammen oder diesem zur Verfügung zu stellen sind, auf Verlangen des Auftraggebers heraus oder löscht sie, sofern keine gesetzliche Aufbewahrungspflicht besteht. Bestehen gesetzliche oder vertragliche Aufbewahrungsfristen, erfolgt eine Sperrung der Daten bis zum Ablauf der Aufbewahrungsfrist; anschließend werden die Daten gelöscht. Der Auftragnehmer bestätigt dem Auftraggeber die Löschung auf Anfrage. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

§ 4 Pflichten des Auftraggebers

(1) Im Falle einer Inanspruchnahme des Auftragnehmers durch eine betroffene Person hinsichtlich etwaiger Schadensersatzansprüche nach Art. 82 DSGVO, gilt § 3 Abs. 4 entsprechend.

(2) Der Auftraggeber nennt dem Auftragnehmer einen Kontakt für im Rahmen der Vereinbarung anfallende Datenschutzfragen. Der Auftraggeber trägt Sorge für die Aktualität dieser Informationen

§ 5 Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Anträgen auf Wahrnehmung der in Kapitel III DSGVO genannten Rechte an den Auftragnehmer, wird der Auftragnehmer die betroffene Person unverzüglich an den Auftraggeber verweisen und leitet den Antrag an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten TOM bei seiner Pflicht zur Beantwortung dieser Anträge der betroffenen Personen auf Weisung. Der Auftragnehmer kann hierfür eine Vergütung verlangen, sofern diese Leistungen nicht bereits aufgrund des Vertrages abgegolten sind. Auskünfte an Dritte darf der Auftragnehmer nicht erteilen,

es sei denn, er ist nach dem Unionsrecht oder dem Recht eines Mitgliedstaats zur Herausgabe der Auskunft verpflichtet; in dem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtliche Anforderung vor der Auskunftserteilung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

§ 6 Nachweismöglichkeiten

(1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die dokumentierten Kontrollen und erforderlichen Auskünfte zur Verfügung zu stellen. Insbesondere ist die Umsetzung der technischen und organisatorischen Maßnahmen gemäß Art 32 DSGVO nachzuweisen.

(2) Der Nachweis der Einhaltung der in diesem Vertrag niedergelegten Pflichten kann erfolgen durch

a. aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren)
b. Selbstaudits
c. eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz, ISO 27001, ISO 27018, ISO 27701)
d. die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO
e. die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO

(3) Kontrollrechte

a. Auf Verlangen des Auftraggebers gestattet der Auftragnehmer die Prüfung der unter diese Vereinbarung fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung kann der Auftraggeber die im vorherigen Absatz genannten Zertifizierungen des Auftragnehmers berücksichtigen. Der Auftraggeber kann die Überprüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen.
b. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragnehmers umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt. Bei Vor-Ort-Inspektionen müssen die Vertraulichkeitsinteressen des Auftragnehmers beachtet werden. Dies kann den Abschluss einer Geheimhaltungsverpflichtung beinhalten, wobei diese dem Auftraggeber den Nachweis gegenüber der Aufsichtsbehörde und ggf. den Betroffenen in dem erforderlichen Umfang nicht beeinträchtigen darf
c. Eine Prüfung kann insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch weitere Maßnahmen erfolgen. Zu den weiteren Maßnahmen zählen die Anforderung von Zertifizierungen, Berichte zu Datenschutzaudits und Inspektionen vor Ort. Inspektionen vor Ort nimmt der Auftraggeber mit angemessener Vorankündigung während der üblichen Geschäftszeiten vor. Die Prüfungen müssen ohne Störung des

Betriebsablaufs sowie unter Wahrung der Sicherheits- und Vertraulichkeitsinteressen des Auftragnehmers durchgeführt und ist auf eine Prüfung pro Kalenderjahr beschränkt. Ausgenommen sind anlassbezogene Kontrollen. Jede Partei trägt die ihr entstandenen Kosten der Prüfungen in den vorgenannten Fällen (incl. Nachprüfungen) selbst.

§ 7 weitere Auftragsverarbeiter (Subunternehmer)

(1) Die in der Anlage 3 zu dieser Vereinbarung aufgeführten Subunternehmer gelten als genehmigt. Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer Subunternehmer mit im Vertrag vereinbarten Verarbeitungen personenbezogener Daten beauftragt. Der Auftragnehmer wird mit diesen Subunternehmern im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.

(2) Der Auftragnehmer darf Subunternehmer nur unter folgenden Voraussetzungen einsetzen: Der Auftraggeber erteilt dem Auftragnehmer eine allgemeine Genehmigung zum Einsatz von Subunternehmern. Der Auftragnehmer informiert den Auftraggeber vor Hinzuziehung oder Ersetzung eines Subunternehmers schriftlich bzw. per E-Mail. Der Auftraggeber kann der Hinzuziehung oder Ersatz innerhalb einer angemessenen Frist von mindestens 14 Kalendertagen aus wichtigem datenschutzrechtlichem Grund widersprechen. Erfolgt kein Widerspruch innerhalb der Frist, gilt die Zustimmung als erteilt.
Für Notfallsituationen, z. B. bei dringendem Sicherheitsrisiko oder unvorhergesehenem Ausfall eines Subunternehmers, darf der Auftragnehmer einen Subunternehmer auch ohne Einhaltung der oben genannten Frist hinzuziehen oder ersetzen. In einem solchen Fall informiert der Auftragnehmer den Auftraggeber unverzüglich über die Änderung.

(3) Der Auftragnehmer stellt dem Auftraggeber eine aktuelle Liste aller eingesetzten Subunternehmer zur Verfügung. Diese Liste wird als Anlage 3 zum Vertrag beigefügt.

(4) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer dem Subunternehmer entsprechend Art. 28 Abs. 4 DSGVO, dieselben datenschutzrechtlichen Pflichten aus dieser Vereinbarung zu übertragen. Der Auftragnehmer stellt sicher, dass der Subunternehmer die Pflichten erfüllt, denen der Auftragnehmer entsprechend dieser Vereinbarung und den Bestimmungen der DSGVO unterliegt. Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, haftet der Auftragnehmer in vollem Umfang gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Subunternehmers.

§ 8 Übermittlung in Drittstaaten

(1) Eine Übermittlung findet nur auf dokumentierte Weisung des Verantwortlichen in Drittstaaten außerhalb der EU und des EWR statt, sofern die Voraussetzungen nach Art. 44ff DSGVO eingehalten werden.

(2) Die Vertragsparteien legen in dieser Vereinbarung die jeweils einschlägigen Mechanismen zur Sicherstellung eines angemessenen Schutzniveaus fest. Das angemessene Schutzniveau wird, soweit einschlägig, gewährleistet durch:

a. Einen Angemessenheitsbeschluss der EU-Kommission (Art. 45 DSGVO);

b. den Abschluss von Standarddatenschutzklauseln der EU – Kommission gemäß Art. 46 Abs. 2 lit. c, d DSGVO in ihrer jeweils aktuellen Fassung sowie, soweit erforderlich, zusätzliche TOM

c. verbindliche interne Datenschutzvorschriften (BCR) i.S.d. Art 46 Abs. 2 lit. b, Art. 47 DSGVO

d. genehmigte Verhaltensregeln oder Zertifizierungsmechanismen gemäß Art. 46 Abs. 2 lit. e, f DSGVO

Das angemessene Schutzniveau wird primär durch einen Angemessenheitsbeschluss gemäß Art. 45 DSGVO gewährleistet. Nur sofern ein solcher nicht besteht, kommen die weiteren Mechanismen zur Anwendung. Sofern der Abschluss von Standarddatenschutzklauseln erfolgt und kein Angemessenheitsbeschluss vorliegt, verpflichtet sich der Auftragnehmer, ein Transfer Impact Assessment (TIA) nach Vorgaben der EU-Kommission und der Aufsichtsbehörden durchzuführen und zu dokumentieren. Hierbei sind zusätzliche technische, organisatorische und vertragliche Maßnahmen zu ergreifen, wenn dies zur Herstellung eines angemessenen Datenschutzniveaus geboten ist. Das TIA sowie getroffene Zusatzmaßnahmen werden dem Auftraggeber auf Anfrage zur Verfügung gestellt.

(3) Ist hierzu nichts im Vertrag vereinbart, ist die Verarbeitung in einem Drittstaat sowohl für den Auftragnehmer als auch seine Subunternehmer nur mit vorheriger Zustimmung des Auftraggebers zulässig. Der Auftragnehmer teilt dem Auftraggeber vorab mit, um welche(n) Drittstaat(en) es sich handelt und auf welche Weise das angemessene Schutzniveau im Sinne von Art. 44 ff. DSGVO für die Verarbeitung dort sichergestellt ist. Im Fall der Hinzuziehung eines Subunternehmers in einem Drittstaat gilt die Genehmigung nach § 7 auch als Genehmigung nach diesem § 8.

§ 9 Haftung

Die Haftung richtet sich nach dem abgeschlossenen Hauptvertrag. Die Haftung nach Art. 82 DSGVO bleibt hiervon unberührt, soweit sie gegenüber betroffenen Personen zwingend gesetzlich vorgeschrieben ist.

§ 10 Informationspflichten, Schriftformklausel, Rechtswahl

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher« im Sinne der Datenschutz-Grundverordnung liegen.

(2) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht. Die Vertragsparteien vereinbaren und gestatten der jeweils anderen Vertragspartei, Informationen aus dieser Vereinbarung zum Zweck der Abwehr von Ansprüchen Dritter und zum Zweck des Nachweises, dass die jeweilige Vertragspartei in keinerlei Hinsicht für den Umstand, durch den ein Schaden eingetreten ist, verantwortlich ist, zu nutzen.

(4) Es gilt deutsches Recht.

Anlagen

Anlage 1 – Art der Daten und Kreis der Betroffenen

Anlage 2 – Technische und organisatorische Maßnahmen des Auftragnehmers

Anlage 3 – Genehmigte Subunternehmer

Anlage 1: Art der Daten und Kreis der Betroffenen

1. Art der verarbeiteten personenbezogenen Daten

Im Rahmen der Erbringung der Leistungen aus dem Hauptvertrag verarbeitet der Auftragnehmer die folgenden Datenkategorien:

- Stamm- und Kontaktdaten des Auftraggebers/Partners: Namen, Anschrift, E-Mail-Adresse von B2B-Ansprechpartnern.
- Stamm- und Kontaktdaten des Nutzers: Name, Vorname, Anschrift, E-Mail-Adresse, Telefonnummer.
- Daten von Vertrauenspersonen: Namen und E-Mail-Adressen der vom Nutzer in der Plattform benannten Begünstigten oder Bevollmächtigten.
- Vertrags- und Abrechnungsdaten: Zahlungsinformationen, gewählte Pakete und Buchungshistorie.
- Verschlüsselte Inhaltsdaten: Digitale Dokumente (z. B. Urkunden, Testamente), Zugangsdaten, Passwörter und persönliche Anweisungen, die der Nutzer auf der Plattform hinterlegt.
- Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO): Sofern vom Nutzer eigenverantwortlich hinterlegt, können die Dokumente auch Gesundheitsdaten (z. B. Patientenverfügungen) oder religiöse Informationen enthalten.
- Nutzungs- und Metadaten: IP-Adressen, Login-Zeitstempel und technische Protokolldaten zur Sicherstellung der Systemintegrität.

2. Kreis der von der Datenverarbeitung Betroffenen

Die Verarbeitung betrifft die folgenden Gruppen von Personen:

- Nutzer der Plattform: Personen, die als Vertragspartner ein Konto bei dem Auftragnehmer führen.
- Kunden der Partner: Personen, deren Vorsorge über einen Partner (z. B. Steuerberater) beim Auftragnehmer verwaltet wird.
- Vertrauenspersonen / Begünstigte: Personen, die vom Nutzer als Empfänger für Datenfreigaben im Vorsorgefall bestimmt wurden.
- Beschäftigte des Auftraggebers: Ansprechpartner beim Partnerunternehmen, die das System verwalten

Anlage 2: Technische und organisatorische Maßnahmen des Auftragnehmers zum Datenschutz gemäß Art. 32 DSGVO

Der Auftragnehmer ist verpflichtet, nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit im Sinne des Art. 32 DSGVO einzuhalten.

Die Plattform wird vollständig in Rechenzentren der Scaleway SAS in der Europäischen Union betrieben (Produktivsystem in Amsterdam, Niederlande; Datensicherungen in Paris, Frankreich). Der Auftragnehmer betreibt keine eigenen Serverräume.

1. Organisatorische Maßnahmen

X Alle Mitarbeiter sind nachweislich auf die Vertraulichkeit (Datengeheimnis), ggf. auf das Fernmeldegeheimnis und die Wahrung von Berufsgeheimnissen, verpflichtet

X Dokumentierte Betriebs- und Notfallverfahren (Runbooks) für Betrieb, Wiederherstellung und Sicherheitsvorfälle

2. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

X Physische Zutrittskontrolle zu den Rechenzentren durch den Hosting-Dienstleister Scaleway SAS nach dessen technischen und organisatorischen Maßnahmen (Anlage 3)

X Büroräume: Alarmanlage, Türsicherung (elektrischer Türöffner, Zahlenschloss usw.)

2.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

X Passwortvergabe, Authentifikation mit Benutzername/Passwort

X Komplexität des Passworts + OTP (2-Faktor-Authentifizierung)

X Anzahl der Fehleingaben beschränkt

X Automatische Sperrung des Arbeitsplatzes

X Anmeldung an der Plattform über einen spezialisierten Authentifizierungsdienst (Auth0, EU-Region) mit Mehr-Faktor-Authentifizierung

X Schutz der Formulare und Anmeldeseiten vor automatisierten Angriffen (Friendly Captcha)

X Erkennung und automatische Sperrung angreifender IP-Adressen (Intrusion Prevention mit CrowdSec)

2.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

X Zuordnung von Benutzerrechten / Erstellen von Benutzerprofilen

X Prüfung jedes Zugriffs auf Plattformdaten über zentrale Berechtigungsregeln (Policy-Engine) mit Protokollierung der Entscheidungen

X Verwaltung der Rechte durch System-Administrator

X Anzahl der Administratoren auf das „Notwendigste" begrenzt

X Verschlüsselung von Datenträgern; serverseitige Verschlüsselung aller Speicher-Buckets

X Verwaltung von Zugangsschlüsseln und Passwörtern der Systeme in einem zentralen Secret-Manager, nicht im Quellcode

2.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

X Logische Mandantentrennung (softwareseitig)

X Trennung von Produktiv- und Testsystem (getrennte Umgebungen, Datenbanken und Speicher)

X Festlegung von Datenbankrechten

2.5 Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass der Personenbezug von Daten nicht vollständig, aber immerhin so weit aufgelöst wird, dass ein Rückschluss auf eine bestimmte Person nur unter „Hinzuziehung zusätzlicher Informationen", insbes. eines Identifizierungsschlüssels, möglich ist.

X ja

2.6 Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten durch kryptografische Maßnahmen so verändert werden, dass sie – insbes. während ihres Übertragungsvorgangs – ohne den Schlüssel nicht mehr lesbar sind, ein unberechtigter Zugriff Dritter mithin ausgeschlossen ist.

X ja

X Transportverschlüsselung (TLS/HTTPS) für alle Verbindungen zur Plattform

X Erzwungene TLS-Verschlüsselung der Verbindungen zu Datenbank und Cache

X Serverseitige Verschlüsselung der gespeicherten Dateien

X Verschlüsselte Datensicherungen

3. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

3.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

X Verschlüsselte Übertragung (TLS)

X Firewall; Netzwerkrichtlinien nach dem Prinzip „alles verboten, was nicht ausdrücklich erlaubt ist" für die Kommunikation zwischen den Diensten

X Weitergabe von Daten in anonymisierter oder pseudonymisierter Form bzw. Verschlüsselung

X Protokollierung von Übermittlungen

3.2 Eingabekontrolle/Verarbeitungskontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

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

X Revisionssichere Archivierung der Audit-Protokolle (unveränderbar gespeichert für 4 Jahre)

3.3 Dokumentationskontrolle

Maßnahmen, die gewährleisten, dass die Verfahrensweisen bei der Verarbeitung personenbezogener Daten in einer Weise dokumentiert werden, dass sie in zumutbarer Weise nachvollzogen werden können.

X Dokumentation der eingesetzten IT-Systeme und deren Systemkonfiguration (versionierte Infrastruktur-Konfiguration)

X Zulässigkeit eines Datentransfers in Drittländer ist gegeben

3.4 Auftragskontrolle

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

X Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

X Verträge zur Auftragsverarbeitung mit allen Subunternehmern (Anlage 3)

4. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

4.1 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

X Testen von Datenwiederherstellung

X Backups: tägliche Sicherung der Plattform sowie mehrmals täglich Sicherungen der Datenbank; verschlüsselte Ablage in einer zweiten Region (Paris); Schutz der Sicherungen gegen Löschen und Verändern für 30 Tage (Object Lock)

X Virenschutzsystem; Virenprüfung hochgeladener Dateien

X Konzept für Katastrophenfall vorhanden

4.2 Belastbarkeit (Widerstandsfähigkeit/ Resilienz von Systemen/ Diensten)

Maßnahmen, die gewährleisten, dass technische Systeme, bei Störungen bzw. Teil Ausfällen nicht vollständig versagen, sondern wesentliche Systemdienstleistungen aufrechterhalten werden.

- **X** Redundante Systemauslegung
- **X** Ausfallsicherheits-/Hochverfügbarkeitskonzept
- **X** Einsatz fehlertoleranter Software
- **X** Schutz vor Überlast und Denial of Service-Angriffen
- **X** Überwachung der Systeme mit automatischer Alarmierung sowie Erkennung von Angriffen und verdächtigem Verhalten zur Laufzeit (CrowdSec, Falco)

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

- **X** Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)
- **X** Regelmäßige Sicherheitsüberprüfungen der Infrastruktur
- **X** Automatische Prüfung der Konfiguration auf Abweichungen vom Sollzustand
- **X** Regelmäßige Schwachstellenscans der eingesetzten Software

Anlage 3: Liste der genehmigten Subunternehmer

#	Name und Anschrift des Subunternehmers	Beschreibung der Teilleistung	Ort der Datenverarbeitung
1	Lettermint B.V., Willemsvaart 16 B, 8019 AB Zwolle, Niederlande	Versand automatisierter Mails	Niederlande (EU)
2	Okta (auth0), 100 First Street, San Francisco California 94105, USA*	Authentifizierungsprovider	EU-Region: Frankfurt am Main, Deutschland (Ausweichstandort Dublin, Irland)
3	Scaleway SAS, 8 rue de la Ville-l'Évêque, 75008 Paris, Frankreich	Hosting der Plattform (Cloud-Infrastruktur, Datenbanken, Dateispeicher, Datensicherungen, Protokollierung)	Amsterdam, Niederlande; Paris, Frankreich
4	sentry.io, Functional Software, Inc. dba Sentry, Attn: Legal Department, 45 Fremont Street, 8th Floor, San Francisco, CA 94105-2250, USA*	Bug-Tracker und Monitoring	EU-Region: Frankfurt am Main, Deutschland
5	Rote Robben GmbH, Charlottenstr. 25, 66119 Saarbrücken, Deutschland	Webanalyse der Plattform (Matomo)	Karlsruhe, Deutschland
6	Stripe Technology Company Limited (STC), One Wilton Park, Wilton Place, Dublin 2, D02 FX04, Ireland*	Zahlungsanbieter	Dublin, Irland (AWS)
7	Friendly Captcha GmbH, Am Anger 3-5, 82237 Wörthsee, Deutschland	Captcha/Bot-Schutz	Gunzenhausen, Deutschland (Hetzner)
8	Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland*	E-Mail-Postfächer einschließlich Support-Kommunikation (Microsoft 365)	EU

*Die Datenübermittlung erfolgt auf Grundlage des Angemessenheitsbeschlusses der EU-Kommission vom 10.07.2023 gemäß Art. 45 DSGVO. Der Dienstleister ist zum Zeitpunkt der Datenverarbeitung aktiv nach dem EU-U.S. Data Privacy Framework (DPF) zertifiziert. Die Zertifizierung wird regelmäßig überprüft. Bei Dienstleistern mit Datenverarbeitung in der EU betrifft dies nur Zugriffe aus den USA, etwa im Rahmen von Support und Wartung.