Vertrag über die Verarbeitung personenbezogener Daten

– nachfolgend **„Vertrag“** genannt –

zwischen

dem im Angebot spezifizierten Unternehmen

– nachfolgend **„Auftraggeber“** oder **„Verantwortlicher“** –

und

Zive GmbH
Große Bleichen 1-3
20354 Hamburg
Deutschland

– nachfolgend **„Auftragnehmer“** oder **„Auftragsverarbeiter“** –

einzeln oder gemeinsam auch **„Partei“** und / oder **„Parteien“**

Version vom 25.9.2025

1. Rechtsgrundlage, Gegenstand, Dauer des Vertrages

1.1. Dieser Vereinbarung liegen die Bestimmungen der EU-Datenschutzgrundverordnung (DSGVO) zu Grunde.

1.2. Gegenstand dieses Vertrages ist die Erhebung und Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Verantwortlichen in dessen Auftrag und nach dessen Weisung im Zusammenhang mit den jeweiligen Bedingungen der Cloud-Dienste. Zweck der Auftragsverarbeitung ist die Bereitstellung und Betriebsführung der Software sowie deren Sicherstellung gemäß der Leistungsbeschreibung im Annex 1. Art und Umfang der Verarbeitung, der personenbezogenen Daten sowie die Kategorien betroffener Personen ergeben sich ebenso aus Annex 1.

1.3. Die Dauer dieses Vertrages richtet sich nach der Dauer des Bestehens eines Verarbeitungszweckes gem. Abs. 2 dieser Ziffer, sofern sich aus den nachfolgenden Bestimmungen nicht ein anderes ergibt. Das Recht zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt.

2. Rechte und Pflichten des Verantwortlichen

2.1. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenübermittlung an den Auftragnehmer sowie für die Wahrung der Rechte der betroffenen Personen verantwortlich.

2.2. Der Auftragnehmer wird personenbezogene Daten nur auf dokumentierte Weisung des Auftraggebers — auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation — verarbeiten, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, zu der Verarbeitung verpflichtet ist. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Ist der Auftragnehmer der Ansicht, dass eine Weisung gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

2.3. Der Auftragnehmer wird nur ausreichend qualifizierte und zuverlässige Kräfte mit der Datenverarbeitung betrauen. Insbesondere wird der Auftragnehmer die Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, auf die Wahrung des Datengeheimnisses (Verschwiegenheitspflicht) verpflichten und über die sich aus der Datenverarbeitung ergebenden Datenschutzpflichten sowie bestehende Weisungs- bzw. Zweckbindung belehren.

2.4. Der Auftragnehmer bestellt einen Datenschutzbeauftragten, der in der jeweils aktuellen und öffentlich verfügbaren Datenschutzerklärung des Auftragnehmers bekannt gemacht wird.

2.5. Die Parteien unterstützen sich gegenseitig, zeitnah und umfänglich bei der Prüfung möglicher Verstöße und der Abwehr von Ansprüchen betroffener Personen oder Dritter sowie der Abwehr von Sanktionen durch Aufsichtsbehörden. Der Auftragnehmer unterstützt den Auftraggeber insbesondere dabei, dessen Aufgaben nach den Art. 32 bis 36 DSGVO zu erfüllen sowie dessen Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte betroffener Personen nachzukommen.

2.6. Der Auftragnehmer stellt dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist jederzeit alle verfügbaren Auskünfte und Nachweise bereit, die zur Beurteilung der Vertragsgemäßheit der Datenverarbeitung erforderlich sind. Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von der Einhaltung der in diesem Vertrag vereinbarten Regelungen zum Schutz der personenbezogenen Daten, insbesondere von der Einhaltung der vereinbarten technischen und organisatorischen Maßnahmen des Auftragnehmers und dokumentiert dieses Ergebnis. Hierfür kann er beispielsweise

a. Selbstauskünfte des Auftragnehmers einholen,

b. sich ein Testat eines Sachverständigen bzw. Zertifikate vorlegen lassen oder

c. nach rechtzeitiger Anmeldung zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs persönlich oder durch einen sachkundigen Dritten, der nicht in einem Wettbewerbsverhältnis zum Auftragnehmer stehen darf, von der Einhaltung der vereinbarten Regelungen überzeugen.

2.7. Bei Verdacht auf Verletzungen vertraglicher Verpflichtungen des Auftragnehmers bzw. der bei ihm zur Auftragsverarbeitung beschäftigten Personen oder sonstigen Verstößen gegen datenschutzrechtliche Bestimmungen wird der Auftragnehmer den Auftraggeber unverzüglich in Textform informieren.

3. Technische und organisatorische Maßnahmen

3.1. Der Auftraggeber und der Auftragnehmer werden geeignete technische und organisatorische Maßnahmen (TOM) zur Sicherung der Daten des Auftraggebers vor Missbrauch und Verlust treffen, sodass ein den einschlägigen datenschutzrechtlichen Bestimmungen – insbesondere der DSGVO – angemessenes Schutzniveau gewährleistet werden kann.

3.2. Die von den Parteien zum Zwecke dieser Vereinbarung als geeignet befundenen TOM des Auftragnehmers sind in Annex 2 aufgeführt und beschrieben.

3.3. TOM unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternativ adäquate Maßnahmen umzusetzen. Dabei muss sichergestellt sein, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind abzustimmen und zu dokumentieren.

4. Rückgabe und Löschung

4.1. Der Auftragnehmer wird dem Auftraggeber auf dessen Anforderung alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder löschen, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Dies betrifft auch etwaige Testdaten. Die Parteien werden sich nach dem Herausgabeverlangen auf weitere Modalitäten der Rückgabe (z.B. Format, Frist) einigen.

5. Unterauftragsverarbeiter

5.1. Die vertraglich vereinbarten Leistungen werden unter Einschaltung der in Annex 3 genannten Unterauftragsverarbeiter durchgeführt. Der Auftragnehmer ist im Rahmen dieses Vertrages zur Begründung von weiteren Unterauftragsverhältnissen zur Leistungserbringung befugt.

5.2. Der Auftragnehmer wählt Unterauftragsverarbeiter sorgfältig nach deren Eignung und Zuverlässigkeit aus. Der Auftragnehmer ist verpflichtet, die Unterauftragsverarbeiter entsprechend dieser Vereinbarung zu verpflichten. Er stellt insbesondere sicher, dass der Verantwortliche seine Rechte aus dieser Vereinbarung auch direkt gegenüber den Unterauftragsverarbeitern wahrnehmen kann, die Unterauftragsverarbeiter hinreichende Garantien dafür bieten, dass sie denselben Datenschutzpflichten unterliegen wie der Auftragnehmer und die TOM der Unterauftragsverarbeiter so durchgeführt werden, dass sie den Anforderungen dieser Vereinbarung entsprechen. Der Auftragsverarbeiter hat dem Verantwortlichen auf dessen schriftliche Aufforderung Auskunft über die datenschutzrelevanten Verpflichtungen des Unteraufragnehmers zu erteilen. Dies umfasst erforderlichenfalls auch die Einsicht in die relevanten Vertragsunterlagen.

5.3. Der Auftragnehmer informiert den Verantwortlichen per E-Mail über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung von Unterauftragsverarbeitern, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen binnen 14 Tagen wegen eines wichtigen Grundes Einspruch zu erheben. Dem Auftragnehmer steht ein außerordentliches Kündigungsrecht zu, wenn der Verantwortliche der Einbindung des Unterauftragsverarbeiters ohne wichtigen Grund widerspricht.

5.4. Als Unterauftragsverarbeiter gelten auch Auftragsverarbeiter des Unterauftragsverarbeiters (Sub-Unterauftragsverarbeiter). Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Aufträge zu verstehen, die der Auftragsverarbeiter Dritten zur Unterstützung bei der Auftragsdurchführung erteilt und die keine Verarbeitungsleistungen von Daten des Verantwortlichen beinhalten. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind insbesondere Nebenleistungen zu verstehen, die der Anbieter z.B. als Telekommunikationsleistung, Post-/Transportdienstleistung, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahme zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt.

5.5. Die Übermittlung personenbezogener Daten in Länder außerhalb des EWR darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B.

durch Einhaltung des EU Data Privacy Frameworks oder die Übernahme von Standardvertragsklauseln, die von der Europäischen Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 in ihrer Fassung vom 4. Juni 2021 angenommen wurden.

6. Haftung

6.1. Für den Ersatz von Schäden, die ein Betroffener wegen einer nach der DSGVO oder anderen Vorschriften für den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, ist der Auftraggeber gegenüber dem Betroffenen verantwortlich. Soweit der Auftraggeber zum Schadenersatz verpflichtet ist, bleibt ihm der Rückgriff beim Auftragnehmer vorbehalten, soweit Pflichten aus diesem Vertrag verletzt wurden.

6.2. Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist.

7. Sonstiges

7.1. Diese Vereinbarung zur Auftragsverarbeitung löst sämtliche vorangegangenen Regelungen zur Auftragsverarbeitung.

7.2. Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam oder undurchführbar erweisen oder nach Vertragsabschluss unwirksam oder undurchführbar werden, bleiben die übrigen Vertragsbestimmungen und die Wirksamkeit des Vertrages im Ganzen hiervon unberührt. An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll eine wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung bzw. dem von den Parteien Gewollten am nächsten kommt.

7.3. Es gilt deutsches Recht einschließlich europäisches Recht wie die DSGVO. Gerichtsstand ist Hamburg, Deutschland.

7.4. Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile bedürfen einer schriftlichen Vereinbarung.

Einzelheiten zur Datenverarbeitung der Software Zive

Leistungsbeschreibung

Zive ist eine moderne Plattform für KI- und Wissensmanagement in Firmen. Ziel der Anwendung ist es, den Mitarbeitern des Kunden eine einheitliche und sichere KI-Arbeitsumgebung bereitzustellen.

Weitere Informationen zu Art und Umfang der Software gehen aus Angebot und Leistungsbeschreibung hervor.

Einzelheiten über die Datenverarbeitung

Beschreibung der Verarbeitungstätigkeit

Im Wesentlichen handelt es sich um folgende Aufgaben durch den Auftragnehmer:

- Bereitstellung der Software, die dem internen Wissensmanagement dient.
- Hosting von Daten des Auftraggebers auf einer IT-Infrastruktur, die vom Auftragnehmer und seinen Erfüllungsgehilfen bereitgestellt wird.

Betroffenenkategorien, Datenarten, Zugriffsformen

a. Kategorien betroffener Personen

Grundsätzlich dient die Software dem internen Wissensmanagement. Soweit durch den Kunden (Verantwortlicher) beabsichtigt ist, personenbezogene Daten weiterer Kategorien in der Software zu verarbeiten, wäre dies nachfolgend durch den Verantwortlichen zu kennzeichnen.

- ☑ Beschäftigte
- ☑ Kunden
- ☑ Lieferanten
- ☐ Handelsvertreter
- ☐ Interessenten
- ☐ Ansprechpartner obiger Kategorien

b. Betroffene personenbezogene Daten

Zur Nutzung der Software ist nur die Angabe von Name und E-Mail-Adresse notwendig. Darüber hinaus greift die Software auf öffentliche Stammdaten der Mitarbeiter zu. Soweit der Kunde (Verantwortliche) weitere Datenarten in der Software verwenden möchte, so ist dies durch weitere Kreuze durch den Verantwortlichen kenntlich zu machen.

- ☑ Nachname/Vorname
- ☑ Profilfoto
- ☐ Anschrift
- ☐ Geburtsort
- ☐ Familienstand
- ☑ Kontaktdaten (z.B. Telefon, E-Mail)
- ☐ Anschrift
- ☐ Unterschrift
- ☑ Bestandsdaten (z.B. Rechnungsanschrift, Vertragsnummer)
- ☐ Verkehrsdaten (z.B. Anschlusskennung, Standortdaten, Anfang/Ende einer Telefonverbindung)
- ☑ Vertragsstammdaten
- ☐ Personalstammdaten
- ☑ Kommunikationsdaten
- ☐ Abrechnungsdaten
- ☑ Kundenhistorie
- ☐ Nationalität
- ☑ Beruf
- ☐ Bankkonto
- ☐ sonstiges:

c. Sensible Daten / Besondere Kategorien von Daten i.S.v. Art. 9 DSGVO

Zur Nutzung der Software werden keine sensiblen Daten benötigt. Soweit der Verantwortliche sensible Daten in der Software verarbeiten möchte, so ist dies durch den Verantwortlichen zu ergänzen.

d. Zugriff auf personenbezogene Daten

Der Auftragsverarbeiter erbringt Leistungen im Bereich des Hostings, jedoch auch der Wartung, Fernwartung oder IT-Fehleranalyse. Hierbei kann die Möglichkeit, dass der Auftragsverarbeiter Zugriff auf die Daten erhält, nicht ausgeschlossen werden. Dafür gelten folgende, erweiterte Pflichten:

- Der Auftragsverarbeiter wird von den ihm eingeräumten Zugriffsrechten – auch in zeitlicher Hinsicht – so wenig Gebrauch machen, als dies für die ordnungsgemäße Durchführung der beauftragten Wartungs- und Prüfungsarbeiten notwendig ist.

- Es erfolgt eine gesonderte Mitteilung (per Mail/schriftlich) über anstehende Prüfungs- und Wartungsarbeiten durch den Auftragsverarbeiter an den Verantwortlichen vor Beginn der Arbeiten.
- Auf Anforderung des Verantwortlichen informiert der Auftragsverarbeiter, welche Arbeiten wann durchgeführt werden.

Technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung

Die Zive GmbH sichert zu, folgende technische und organisatorische Maßnahmen getroffen zu haben:

A. Maßnahmen zur Pseudonymisierung

Maßnahmen, die den unmittelbaren Personenbezug während der Verarbeitung in einer Weise reduzieren, dass nur mit Hinzuziehung zusätzlicher Informationen eine Zuordnung zu einer spezifisch betroffenen Person möglich ist. Die Zusatzinformationen sind dabei durch geeignete technische und organisatorische Maßnahmen von dem Pseudonym getrennt aufzubewahren.

- Pseudonymisierung wird überall angewendet, wo es möglich ist und die Erfüllung der Leistung des Hauptvertrags nicht eingeschränkt.
- Auswahl eines geeigneten Pseudonymisierungsverfahrens nach aktuellem Stand der Technik.

B. Maßnahmen zur Verschlüsselung

Maßnahmen oder Vorgänge, bei denen ein klar lesbarer Text / Information mit Hilfe eines Verschlüsselungsverfahrens (Kryptosystem) in eine unleserliche, das heißt nicht einfach interpretierbare Zeichenfolge (Geheimtext) umgewandelt wird.

- Alle Daten, die vom Verantwortlichen zum Auftragsverarbeiter übertragen werden, sowie alle Daten, die während der Verarbeitung zwischen Systemen des Auftragsverarbeiters übertragen werden, werden mit Hilfe von TLS 1.2 oder besser verschlüsselt.
- Alle Daten, die auf Datenträgern gespeichert werden, werden mit AES 256 oder besser verschlüsselt.

C. Maßnahmen zur Sicherung der Vertraulichkeit

C1. Zutrittskontrolle

Maßnahmen, die unbefugten Personen den Zutritt zu IT-Systemen und Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, sowie zu vertraulichen Akten und Datenträgern physisch verwehren.

- Trifft nicht zu, da der Auftragsverarbeiter keine eigenen IT-Systeme oder Datenverarbeitungsanlagen betreibt, die personenbezogene Daten verarbeiten.
- Richtlinien für mobiles Arbeiten / Home Office.
- Weiterhin gelten die Maßnahmen der Zutrittskontrolle der eingesetzten Cloud Provider (Subunternehmer), insb. Microsoft Azure EU

- Darüber hinaus gelten die nachfolgend genannten Maßnahmen der Zugangskontrolle, um den unbefugten Zugang zu Systemen zu verhindern, über die ein Zugriff auf die Systeme der Cloud Provider möglich wäre.

C2. Zugangskontrolle

Maßnahmen, die verhindern, dass Unbefugte datenschutzrechtlich geschützte Daten verarbeiten oder nutzen können.

- Kennwortrichtlinie (u.a. Festlegungen hinsichtlich Verwendung von Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts, Verbot der Weitergabe)
- Authentifizierung ausschließlich mit 2FA oder biometrischen Passkeys
- Richtlinien für mobiles Arbeiten / Home Office
- Automatische Sperrung des Bildschirms bei Inaktivität
- Protokollierung der Authentifizierungsversuche und Kontosperrung nach mehrfachen erfolglosen Versuchen
- Ausschließliche Speicherung von Server- und Client Secrets in extra dafür vorgesehen und abgesicherten Schlüsseltresoren (“Key Vault”)
- Einsatz von individuellen Benutzerkonten
- Begrenzung der Zahl der berechtigten Mitarbeiter
- Regelmäßige Überprüfung der Rollen und Zugangslisten
- Verbot des Einsatzes privater Datenträger
- Verschlüsselung von allen Datenträgern (“at rest”)
- Geräteortung und Fernsperre

C3. Zugriffskontrolle

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

- Zugangsberechtigte können nur auf Daten zugreifen, die in dem individuellen Berechtigungsprofil eingerichtet sind
- Der Umfang der Berechtigungen, ist auf das zur jeweiligen Aufgaben- bzw. Funktionserfüllung notwendige Minimum beschränkt (logisch, zeitlich, …)
- Begrenzung der Zahl der berechtigten Mitarbeiter
- Regelmäßige Überprüfung der Rollen und Zugangslisten
- Verwendung von benutzerbezogenen und individualisierten Anmeldeinformationen, insb. Einsatz von individuellen Benutzerkonten
- Kennwortrichtlinie, insb. keine Weitergabe von Kennwörtern
- Verbot des Einsatzes privater Datenträger
- Verschlüsselung von allen Datenträgern (“at rest”)
- Protokollierung des Datenzugriffs:
    - Alle Lese-, Eingabe-, Änderungs- und Löschtransaktionen werden protokolliert (Benutzerkennung, Transaktionsdetails) und für mindestens 6 Monate revisionssicher archiviert

    - Zur Missbrauchserkennung werden regelmäßig stichprobenartige Auswertungen vorgenommen

C4. Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden und so von anderen Daten und Systemen getrennt sind, dass eine ungeplante Verwendung dieser Daten zu anderen Zwecken ausgeschlossen ist.

- Benutzerprofile / Trennung von Nutzerkonten
- Unterschiedliche Zugriffsberechtigungen
- Logisch getrennte Speicherung auf denselben Systemen / Mandantentrennung
- Trennung der verarbeitenden Systeme
- Trennung von Produktiv- und Testsystem
- Keine Produktivdaten in Testsystemen

C5. Weitere Maßnahmen

- Vertraulichkeitsvereinbarungen mit internen und externen Mitarbeitern
- Vertraulichkeitsvereinbarungen mit externen Dienstleistern
- Sicherheitsvereinbarungen mit externen Dienstleistern
- Berücksichtigung der Grundsätze des Datenschutzes durch Technik und der datenschutzfreundlichen Grundeinstellungen (Privacy by Design, Privacy by Default)
- Eingrenzung der zulässigen Personalkräfte auf solche, die nachprüfbar zuständig (örtlich, fachlich), fachlich befähigt, zuverlässig (ggf. sicherheitsüberprüft) und formal zugelassen sind sowie keine Interessenskonflikte bei der Ausübung aufweisen

D. Maßnahmen zur Sicherung der Integrität

D1. Datenintegrität

Maßnahmen, die gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden.

- Verschlüsselung sämtlicher Daten “in transit” und “at rest” (siehe oben)
- Logisch getrennte Speicherung auf denselben Systemen / Mandantentrennung
- Trennung der verarbeitenden Systeme
- Trennung von Produktiv- und Testsystem
- Keine Produktivdaten in Testsystemen
- Vollautomatisierte Releaseprozesse via Versionskontrollsystem
- Automatisierte Testverfahren
- Anwendung des Grundsatzes des geringsten Zugriffsrechts
- Logging (z.B. Serverlogs, Network Flow Logs)

D2. Übertragungskontrolle

Maßnahmen, die gewährleisten, 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.

- Container-basierte Serversysteme (virtuell abgeriegelte Netzwerke)
- Maßnahmen zur Abwehr von Angriffen (z.B. Virenscanner, Firewall)
- Verschlüsselung der Übertragung von Daten, insbesondere bei der Übertragung über öffentliche Netze (z.B. SSL, TLS)
- Verschlüsselung von Datenträgern (“at rest”)
- Einsatz von individuellen Benutzerkonten
- Begrenzung der Zahl der berechtigten Mitarbeiter
- Regelmäßige Überprüfung der Rollen und Zugangslisten
- Logging (z.B. Serverlogs, Network Flow Logs)

D3. Transportkontrolle

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

- Container-basierte Serversysteme (virtuell abgeriegelte Netzwerke, u.a. L2TP, IPSec)
- Verschlüsselung der Übertragung von Daten, insbesondere bei der Übertragung über öffentliche Netze (z.B. SSL, TLS)
- Verschlüsselung von Datenträgern (“at rest”)
- Maßnahmen zur Abwehr von Angriffen (z.B. Virenscanner, Firewall)
- Logging (z.B. Serverlogs, Network Flow Logs, Löschprotokollierung)

D4. Eingabekontrolle

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

- Regelmäßige Überprüfung der Rollen und Zugangslisten
- Audit Trailing aller Konfigurations- und Datenänderungen (z.B. “Azure Activity Logs”)
- Logging (z.B. Serverlogs, Request Logs)

E. Maßnahmen zur Sicherung der Verfügbarkeit und Belastbarkeit

E1. Verfügbarkeitskontrolle

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

- Maßnahmen zur Abwehr von Angriffen (z.B. Virenscanner, Firewall)
- Container-basierte Serversysteme (virtuell abgeriegelte Netzwerke)
- Automatisches Monitoring mit zahlreichen Benachrichtigungskanälen
- Erstellung regelmäßiger Backups nach dem Stand der Technik

- Regelmäßige Durchführung von Penetrationstests
- Weiterhin gelten die Maßnahmen der Verfügbarkeitskontrolle der eingesetzten Cloud Provider (Subunternehmer), insb. Microsoft Azure EU.

E2. Rasche Wiederherstellbarkeit

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

- Verwendung von "Infrastructure as Code" sowie Trennung von Anwendungs- und Datensystemen
- Georedundante Speicherung
- Automatisiertes Wiederherstellungsverfahren
- Bereitschaftsdienst 24/7

E3. Zuverlässigkeit

Maßnahmen, die gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

- Automatisches Load Balancing und automatische Systemskalierung bei Last
- Ausschließliche Zusammenarbeit mit bewährten Cloud Providern, insb. Microsoft Azure EU, die geeignete Backups, Georedundanz und Failover Techniken anwenden
- Automatisches Monitoring mit zahlreichen Benachrichtigungskanälen
- Regelmäßige Durchführung von Penetrationstests
- Verwendung von "Infrastructure as Code" sowie Trennung von Anwendungs- und Datensysteme
- Bereitschaftsdienst 24/7

F. Maßnahmen zur regelmäßigen Evaluation der Sicherheit der Datenverarbeitung

F1. Überprüfungsverfahren

Maßnahmen, die die datenschutzkonforme und sichere Verarbeitung sicherstellen.

- Regelmäßige Überprüfung des Hard- und Softwarebestandes entsprechend einem Bestandsverzeichnis und jährliche Aktualisierung des Bestandsverzeichnisses
- Regelmäßige Überprüfung von Datenverarbeitungssystemen und Verarbeitungstätigkeiten auf Sicherheitslücken, die aufgrund neuer technischer Entwicklungen oder veränderter Verarbeitungspraxis entstehen können
- Regelmäßige Versionskontrolle von Standardsoftware (Intensität der Kontrolle hängt von der eingesetzten Software ab, Prüfung soll jedoch mindestens einmal jährlich erfolgen)
- Regelmäßige Audits mit dem Datenschutzbeauftragten

F2. Auftragskontrolle

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

- Festgelegte Kriterien zur Auswahl der Auftragnehmer (Referenzen, Zertifizierungen, Gütesiegel)
- Gesetzeskonforme Vertragsgestaltung von Verträgen über die Datenverarbeitung personenbezogener Daten mit Subunternehmern mit entsprechender Regelung von Kontrollmechanismen
- Vertragliche Vereinbarung mit Subunternehmern, eigene und externe Mitarbeiter auf das Datengeheimnis zu verpflichten
- Einholung von Selbstauskünften bei Dienstleistern bezüglich deren Maßnahmen zur Umsetzung datenschutzrechtlicher Anforderungen
- Begrenzung der Zahl der berechtigten Mitarbeiter / Benutzerkonten

F3. Incident-Response-Management

Im Falle einer Verletzung des Schutzes personenbezogener Daten ist der Verantwortliche verpflichtet (Art. 33 DSGVO) unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Art. 55 zuständigen Aufsichtsbehörde zu melden, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

Maßnahmen im Datenschutzvorfall:

- Überprüfung von Verdachtsfällen
- Beschreibung des Prozesses, was im Falle einer Datenpanne zu geschehen hat
- Beschreibung der Verantwortlichkeiten
- Beschreibung des technischen Ablaufs zur Beseitigung einer Datenpanne

F4. Weitere Maßnahmen

- Datenschutzfreundliche Voreinstellungen
    - Minimierung der Menge der erhobenen Daten
    - Reduzierung des Umfangs der Datenverarbeitung
    - Reduzierung der Speicherfristen
- Schriftliche Benennung des Datenschutzbeauftragten (DSB)
- Der DSB ist bei der Datenschutzfolgeabschätzung eingebunden
- Datenschutzrechtlich Schulung von Mitarbeitern inkl. Verpflichtung der Mitarbeiter auf Vertraulichkeit beim Umgang mit personenbezogenen Daten
- Rechtliche Verpflichtung von Mitarbeitern zur Einhaltung der internen Sicherheits- und Datenschutzrichtlinien

Information about sub-processors for the Zive software

The following sub-processors may be used under these agreements:

Name	Address	Services	Data process location	International data transfer	Data processing basis (for non-EU)
Microsoft Ireland Operations, Ltd.	One Microsoft Place South County Business Park Leopardstown Dublin 18, D18 P521, Ireland	Cloud compute and AI models	EU	No	Not applicable
Intercom, Inc.	55 2nd Street, 4th Fl., San Francisco, CA 94105, USA	Service and help desk	EU	No	Not applicable
Heureka Labs UG	Haidkoppelweg 27b 21465 Reinbek Germany	AI services	EU	No	Not applicable
Mistral AI*	15 Rue des Halles 75001 Paris, France	AI services	EU	No	Not applicable
Tavily Inc.*	AlphaAI Technologies Inc., dba Tavily 051 Frederick Douglass 5B NY 10026, USA	Web search	USA	Yes	Standard Contractual Clauses (SCCs)

Annex 3

Name	Address	Services	Data process location	International data transfer	Data processing basis (for non-EU)
Google LLC*	1600 Amphitheatre Parkway Mountain View CA 94043, USA	AI models	EU, USA	Yes	EU-U.S. Data Privacy Framework (DPF)
Amazon Web Services Inc.*	410 Terry Avenue North, Seattle, WA 98109-5210, USA	AI models	EU, USA	Yes	Standard Contractual Clauses (SCCs)
Anthropic PBC*	548 Market St, San Francisco, USA	AI models	EU, USA	Yes	Standard Contractual Clauses (SCCs)

* Only applicable when switched on manually by the client in the platform administration.