Vereinbarung zur Auftragsverarbeitung
Artikel 28 DSGVO

Vereinbarung

zwischen

[Name]
[Anschrift]

– Verantwortlicher, nachfolgend „Auftraggeber“ genannt –

und

DigitalErleben GmbH
Ritterstraße 8
33602 Bielefeld

– Auftragsverarbeiter, nachfolgend „Auftragnehmer“ genannt –

Auftraggeber und Auftragnehmer jeweils einzeln als „Partei“ und gemeinsam als „Parteien“ bezeichnet.

---

1. Vertragsgegenstand

Im Rahmen des zwischen den Parteien bestehenden Leistungsverhältnisses über die Bereitstellung und Nutzung der paddy-Plattform (nachfolgend „Hauptvertrag“ genannt) ist es erforderlich, dass der Auftragnehmer als Auftragsverarbeiter i. S. d. Art. 4 Nr. 8 DSGVO mit personenbezogenen Daten umgeht, für die der Auftraggeber Verantwortlicher i. S. d. Art. 4 Nr. 7 DSGVO ist (nachfolgend „Auftraggeber-Daten“ genannt). Dieser Vertrag wird automatisch mit Abschluss des Hauptvertrags geschlossen und konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang des Auftragnehmers mit Auftraggeber-Daten zur Durchführung des Hauptvertrags.

2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten, Kategorien betroffener Personen, Dauer der Auftragsverarbeitung

Der Auftragnehmer verarbeitet die personenbezogenen Daten während der Dauer des Hauptvertrages im Auftrag und nur nach Weisung des Auftraggebers. Art und Zweck der Verarbeitung sowie die Art der personenbezogenen Daten und die Kategorien betroffener Personen werden in **Anlage 1** festgelegt. Jede davon abweichende oder darüber hinaus gehende Verarbeitung von personenbezogenen Daten, insbesondere zu eigenen Zwecken, ist dem Auftragnehmer untersagt.

3. Weisungsrechte des Auftraggebers

3.1 Die Weisungen des Auftraggebers erfolgen grundsätzlich in Schrift- oder Textform (z.B. E-Mail). Abweichend hiervon können (fern-) mündliche Weisungen erfolgen, die im Nachgang in Schrift- bzw. Textform bestätigt werden.

3.2 Der Auftragnehmer ist verpflichtet, die Weisungen des Auftraggebers unverzüglich oder ggf. unter Einhaltung einer durch den Auftraggeber festgelegten, angemessenen Frist auszuführen und insbesondere personenbezogene Daten auf Weisung des Auftraggebers unverzüglich zu berichtigen, zu löschen oder zu sperren und dies auf Verlangen schriftlich zu bestätigen.

3.3 Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen diesen Vertrag, gegen die DSGVO oder gegen andere Datenschutzbestimmungen der EU oder der Mitgliedstaaten verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Ausführung der Weisung bis zu einer Bestätigung oder Änderung der Weisung durch den Auftraggeber auszusetzen.

3.4 Soweit der Auftragnehmer durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, verpflichtet ist, die personenbezogenen Daten auch ohne Weisung des Auftraggebers zu verarbeiten, teilt der Auftragnehmer dem Auftraggeber den Grund der Verarbeitung und die entsprechenden rechtlichen Anforderungen rechtzeitig vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

4. Pflichten des Auftraggebers

4.1 Der Auftraggeber ist nach außen, also gegenüber Dritten und den Betroffenen, für die Rechtmäßigkeit der Verarbeitung der Auftraggeber-Daten sowie für die Wahrung der Rechte der Betroffenen verantwortlich.

4.2 Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebs- und Geschäftsgeheimnissen (insbesondere in Bezug auf technische und organisatorische Maßnahmen der Datensicherheit) des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

4.3 Soweit sich der Auftragnehmer gegen einen Anspruch auf Schadenersatz nach Art. 82 DSGVO, gegen ein drohendes oder bereits verhängtes Bußgeld nach Art. 83 DSGVO oder sonstige Sanktionen im Sinne des Art. 84 DSGVO mit rechtlichen Mitteln verteidigen will, erlaubt der Auftraggeber dem Auftragnehmer Details der Auftragsverarbeitung inklusive erlassener Weisungen zum Zweck der Verteidigung offenzulegen.

5. Pflichten des Auftragnehmers

5.1 Soweit sich eine betroffene Person in Wahrnehmung ihrer Rechte aus Kapitel 3 DSGVO (Art. 12 bis 23 DSGVO) unter Berücksichtigung von Teil 2, Kapitel 2 BDSG (§§ 32 bis 37 BDSG) unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten. Der Auftragnehmer unterstützt den Auftraggeber auf zumutbare Weise mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung solcher Anträge auf Wahrnehmung der in Kapitel 3 DSGVO benannten Rechte der betroffenen Person nachzukommen.

5.2 Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der dem Auftragnehmer zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten.

5.3 Wenn dem Auftragnehmer hinsichtlich der verarbeiteten Auftraggeber-Daten eine Verletzung des Schutzes personenbezogener Daten im Sinne des Art. 4 Nr. 12 DSGVO bekannt wird („Datenschutzvorfall“), meldet er dies dem Verantwortlichen unverzüglich. Im Rahmen der Meldung gem. Art. 33 Abs. 2 DSGVO teilt der Auftragnehmer dem Auftraggeber nach Möglichkeit den Zeitpunkt sowie Art und Ausmaß des Vorfalls, das betroffene IT-System, die betroffenen Personen, den Zeitpunkt der Entdeckung, alle denkbaren nachteiligen Folgen des Datensicherheitsvorfalls sowie die daraufhin ergriffenen Maßnahmen mit.

5.4 Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn Rechte des Auftraggebers an den personenbezogenen Daten beim Auftragnehmer durch Maßnahmen Dritter oder durch sonstige Ereignisse maßgeblich berührt werden.

5.5 Der Auftragnehmer ist verpflichtet, auf Verlangen des Auftraggebers sämtliche Auftraggeber-Daten herauszugeben. Vom Auftraggeber erhaltene Datenträger sind gesondert zu kennzeichnen und laufend zu verwalten. Kopien und Duplikate der personenbezogenen Daten dürfen ausschließlich nach vorheriger Zustimmung durch den Auftraggeber angefertigt werden, sofern sie nicht zur ordnungsgemäßen Durchführung dieser Vereinbarung bzw. des jeweiligen Projektauftrags oder zur Einhaltung von gesetzlichen Aufbewahrungspflichten dienen.

5.6 Sofern eine gesetzliche Pflicht besteht, benennt der Auftragnehmer einen Datenschutzbeauftragten (Art. 37 ff. DSGVO) und teilt dessen Kontaktdaten sowie ggf. den Wechsel des Datenschutzbeauftragten dem Auftraggeber zum Zwecke der direkten Kontaktaufnahme mindestens in Textform mit.

6. Sicherheit der Verarbeitung

6.1 Der Auftragnehmer ergreift alle gemäß Art. 32 DSGVO erforderlichen Maßnahmen, um ein dem Risiko der Verarbeitung angemessenes Schutzniveau zu gewährleisten. Diese Maßnahmen schließen insbesondere die Fähigkeit ein, die Vertraulichkeit, die Integrität, die Verfügbarkeit sowie der Belastbarkeit der Systeme auf Dauer sicherzustellen und die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen. Der Auftragnehmer führt regelmäßig eine Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durch und dokumentiert die Ergebnisse.

6.2 Der Auftragnehmer garantiert, dass er vor Beginn der Verarbeitung der Auftraggeber-Daten die in **Anlage 2** dieses Vertrags aufgelisteten technischen und organisatorischen Maßnahmen implementiert, während der Dauer der Verarbeitung aufrechterhält. Die dokumentierten technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Diese sind durch den Auftragnehmer anzupassen, wenn das bei Vertragsschluss festgelegte Sicherheitsniveau nicht mehr gewährleistet werden kann. Durch die Anpassung muss mindestens das Schutzniveau der bisherigen Maßnahmen erreicht werden. Soweit nichts anderes bestimmt ist, teilt der Auftragnehmer die Anpassungen dem Auftraggeber unaufgefordert mit.

6.3. Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7. Kontrollrechte des Auftraggebers

7.1 Der Auftragnehmer räumt dem Auftraggeber ein Kontrollrecht zur Prüfung der Datenverarbeitung sowie Einhaltung dieses Vertrags bzw. des jeweiligen Projektauftrags ein. Insbesondere stellt der Auftragnehmer dem Auftraggeber alle Informationen zum Nachweis der Einhaltung der in diesem Vertrag niedergelegten Pflichten zur Verfügung und ermöglicht die Durchführung von Überprüfungen einschließlich Inspektionen. Die Kontrollhandlungen können ebenfalls durch einen zur Geheimhaltung verpflichteten Dritten vorgenommen werden, sofern es sich bei dem Dritten um keinen Konkurrenten des Auftragnehmers handelt.

7.2 Die Parteien sind sich einig, dass der Auftraggeber eine Überprüfung nach Ziffer 7.1 durchführt, indem er den Auftragnehmer anweist, nach seiner Wahl ein geeignetes Testat, einen Bericht oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, Informationssicherheitsbeauftragter, Datenschutzauditor oder Qualitätsauditor) oder eine geeignete Zertifizierung durch ein IT-Sicherheits- oder Datenschutzaudit – z.B. nach ISO 27001 oder BSI-Grundschutz – („Prüfungsbericht“) vorzulegen. In begründeten Ausnahmen kann der Auftraggeber eigenständige Inspektionen durchführen.

7.3 Der Auftragnehmer verpflichtet sich, die Durchführung der Kontrollen zu unterstützen. Dies beinhaltet die Gewährung sämtlicher benötigter Zugangs-, Auskunfts- und Einsichtsrechte. Gleiches gilt für öffentliche Kontrollen durch die zuständige Aufsichtsbehörde gemäß den anwendbaren Datenschutzvorschriften.

7.4 Der Auftraggeber hat den Auftragnehmer rechtzeitig (in der Regel mindestens vier Wochen vorher) über alle mit der Durchführung der Kontrolle zusammenhängenden Umstände zu informieren. Der Auftraggeber darf in der Regel eine Kontrolle pro Kalenderjahr durchführen. Hiervon unbenommen ist das Recht des Auftraggebers, weitere Kontrollen im Fall von besonderen Vorkommnissen durchzuführen.

8. Unterauftragsverhältnisse

8.1 Der Auftragnehmer darf Unterauftragsverhältnisse mit weiteren Auftragsverarbeitern (Subdienstleister) begründen. Zurzeit beschäftigt der Auftragnehmer die in **Anlage 3** bezeichneten Subdienstleister. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden. Der Auftragnehmer informiert den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Subdienstleistern, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen innerhalb von zwei Wochen Einspruch zu erheben, wobei dies nicht ohne wichtigen datenschutzrechtlichen Grund erfolgen darf. Sofern der Auftraggeber keine begründeten Einwände innerhalb von 2 Wochen ab Mitteilung über die Änderung erhebt, gilt diese als durch den Auftraggeber genehmigt. Der Auftragnehmer weist den Auftraggeber bei Beginn der Frist auf diese Bedeutung seines Verhaltens hin. Im Fall eines Einspruchs kann der Auftragnehmer nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder – sofern die Erbringung der Leistung ohne die beabsichtige Änderung für den Auftragnehmer nicht zumutbar ist – die Leistung

gegenüber dem Auftraggeber innerhalb von zwei Wochen nach Zugang des Einspruchs einstellen und den Hauptvertrag fristlos und mit sofortiger Wirkung kündigen.

8.2 Ist die Beauftragung eines Subdienstleisters mit einer Übermittlung der Auftraggeber-Daten in ein Land außerhalb der Europäischen Union (EU) oder des Europäischen Wirtschaftsraum (EWR) („Drittland“) verbunden, gelten zusätzlich die Vorgaben aus Ziffer 9.

8.3 Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Datenschutzpflichten, auch gegenüber dem Subdienstleister gelten und diesen gem. Art. 28 Abs. 4 DSGVO vor Aufnahme der Tätigkeiten entsprechend im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats zu verpflichten, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt.

9. Übermittlung von Auftraggeber-Daten an Drittländer

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet grundsätzlich in einem Mitgliedsstaat der Europäischen Union (EU) oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Jede Übermittlung der Auftraggeber-Daten in ein Land außerhalb von EU/EWR („Drittland“) erfolgt nur, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

10. Rückgabe und Löschung von Auftraggeber-Daten

10.1 Der Auftragnehmer hat sämtliche Auftraggeber-Daten nach Abschluss der Erbringung der Verarbeitungsleistungen und insbesondere nach Beendigung der vertragsgegenständlichen Leistungserbringung (insbesondere bei Kündigung oder sonstiger Beendigung des Hauptvertrags) an den Auftraggeber herauszugeben und anschließend datenschutzgerecht zu löschen (inkl. vorhandener Kopien). Von dem Auftraggeber erhaltene Datenträger sind an den Auftraggeber zurückzugeben oder unter Einhaltung einer angemessenen Schutzstufe zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Dies gilt nicht, sofern nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

10.2 Dokumentationen und Protokolle, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung oder gesetzlichen Aufbewahrungsfristen dienen, sind entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

11. Laufzeit und Kündigung

Die Laufzeit und Kündigung dieses Vertrags richten sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrags. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieses Vertrags. Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen.

12. Vorrangklausel

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

Anlagen:
Anlage 1: Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kreis der Betroffenen
Anlage 2: Technische und organisatorische Maßnahmen
Anlage 3: Unterauftragnehmer

Anlage 1: Art und Zweck der Datenverarbeitung, Art der Daten und Kategorien betroffener Personen

Art und Zweck der Datenverarbeitung:

- Bereitstellung einer digitalen Plattform, digitalen Unterrichtsmaterialien
- Speicherung der personenbezogenen Daten in der IT-Infrastruktur
- Verwendung im Rahmen der Bereitstellung innerhalb der Plattform

Art der personenbezogenen Daten:

- Stammdaten (Vorname, Name, Schule/Organisation, Schultyp, Fächer, Rolle, Sprache),
- Kommunikationsdaten (E-Mail-Adresse),
- Nutzungsdaten (IP-Adresse, Browser); durch die Nutzerinnen und Nutzer bereitgestellten Daten (z.B. eingegebene Inhalte)

Kategorien betroffener Personen:

- Lehrkräfte
- Dozent:innen
- Schüler:innen

Anlage 2: Technische und organisatorische Maßnahmen

Verantwortlicher: DigitalErleben GmbH

Datenschutzbeauftragter: Herting Oberbeck Datenschutz GmbH, Herr Sebastian Herting, Hallerstr. 76, 20146 Hamburg, Telefon 040-228691140, datenschutzbeauftragter@digitalerleben.com

Hinweis zu Maßnahmen bei (Unter)-Auftragnehmern:

Die maßgebliche Datenverarbeitung erfolgt auf IT-Systemen, die auf Servern von dem Unterauftragnehmer DigitalOcean LLC betrieben werden. Der Sever befindet sich in Frankfurt am Main (Deutschland). Bitte beachten Sie diesbezüglich ergänzend die vereinbarten technischen und organisatorischen Maßnahmen der DigitalOcean unter https://www.digitalocean.com/legal/data-processing-agreement.

Die Nachfolgend dokumentierten Maßnahmen werden durch den Verantwortlichen umgesetzt.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO) und Verschlüsselung (Art. 32 Abs. 1 lit. a) DSGVO)

Zutrittskontrolle
Maßnahmen, damit Unbefugten der Zutritt zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet werden:

- ☒ Eingangstüren werden stets verschlossen gehalten.
- ☒ Individuelle Zutrittsberechtigung mit Dokumentation der Zutrittsrechte
- ☐ Anwesenheitsaufzeichnungen für Mitarbeiter (Zeiterfassungseinrichtungen)
- ☒ Besucher:innen/Externe werden begleitet bzw. abgeholt und stets beaufsichtigt.
- ☒ Fenstersicherung
- ☒ Chipkarten-/Transponder-Schließsystem
- ☒ Alarmsystem
- ☒ Einzelne IT-Systeme werden in externen Rechenzentren (Hosting) und bei externen Diensten betrieben (Software-as-a-service). Dort gewährleistet der jeweilige Anbieter die Zutrittskontrolle.
- ☐ …

Zugangskontrolle/Verschlüsselung
Maßnahmen, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und -verfahren benutzen:

- ☐ Alle IT-Programme laufen auf dem eigenen Server im Rechenzentrum (Housing)
- ☒ Zugang zu extern gehosteten/betriebenen IT-Systemen ist besonders gesichert (Verschlüsselung, VPN)
- ☐ Abschottung des Netzwerkes gegen ungewollte Zugriffe von außen (Firewall)
- ☒ Zugang zu IT-Systemen nur mit Benutzerkennung und individuellem Passwort möglich; Verwendung eines Passwortmanagers
- ☒ Zugangsberechtigungen werden dokumentiert.
- ☒ Änderung des Passworts nach Sicherheitsvorfall (oder bei Verdacht).
- ☒ stets aktueller Virenschutz.
- ☒ Sperrung der Zugänge nach wiederholten erfolglosen Anmeldeversuchen.
- ☐ Funktionale Zuordnung einzelner Endgeräte und Protokollierung der Systemnutzung.
- ☒ Mobile Datenträger sind verschlüsselt (Hardwareverschlüsselung).
- ☐ Bildschirmsperre an Arbeitsstationen, automatische Sperrung bei längerer Abwesenheit
- ☒ Zwei-Faktor-Identifizierung
- ☐ …

Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können:

☒ Individuelle Zugriffsrechte für alle Benutzer:innen, zentrale Verwaltung und Steuerung.
☒ Zugriffsberechtigungen werden aufgabenbezogen und nach dem Need-to-know-Prinzip erteilt.
☒ Regelmäßige Überprüfung der Zugriffsberechtigungen. Nicht mehr erforderliche Berechtigungen werden unverzüglich entzogen.
☐ Es ist technisch unterbunden, dass Daten auf lokale IT-Systeme kopiert werden.
☒ Daten auf mobilen IT-Systemen sind verschlüsselt (komplettes System, Hardwareverschlüsselung).
☒ Aufzeichnung von Zugriffen auf das IT-System
☐ …

Trennungskontrolle/Zweckbindungskontrolle
Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

☒ Trennung der Zugriffsregelungen über Datenbankprinzip
☒ Softwareseitige Mandantentrennung
☒ Trennung von Produktiv- und Testsystemen (in getrennten Datenbanken)
☐ …

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

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:

☒ Übermittlungen personenbezogener Daten sind im Verzeichnis von Verarbeitungstätigkeiten dokumentiert.
☒ Datenspeicherung und -verarbeitung erfolgt auf IT-Systemen im Rechenzentrum. Verbindung zwischen Clients und Server ist besonders gesichert (Verschlüsselung, VPN).
☒ Kontrollierte Vernichtung von Datenträgern mit Protokollierung (physische Vernichtung, zertifizierter Entsorger)
☒ Besucher:innen haben keinen Zugriff auf betriebliches LAN/WLAN.
☒ sorgfältige Auswahl von Auftragsverarbeitern

Eingabekontrolle
Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt werden können:

☒ automatisierte Protokollierung der Dateneingabe, Änderung oder Löschung
☒ Protokollierung gescheiterter Zugriffsversuche
☒ Protokollierung der Aktivitäten des Systemverwalters und sämtlicher Benutzer:innen
☐ Protokollierung aller Aktivitäten auf dem Server
☒ Sicherung der Protokolldaten gegen Verlust oder Veränderung
☐ …

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b) DSGVO), rasche Wiederherstellbarkeit (Art. 32

Abs. 1 lit. c) DSGVO

Verfügbarkeitskontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (die Angaben beziehen sich auf eigene IT-Systeme des Auftragnehmers):

☒ Datensicherheitskonzept
☒ Versionierte Daten- und Systembackups nach Backup-Plan (täglich/wöchentlich)
☐ Festplattenspiegelung (RAID), Backup-Rechenzentrum
☒ Schadsoftwareschutz
☒ Sicherheitsrelevante Updates und Patches werden regelmäßig und zeitnah eingespielt.
☐ Berichtsverfahren und Notfallplan
☒ Unterbrechungsfreie Stromversorgung
☐ …

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

Auftragskontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftragsgebers verarbeitet werden können:

☒ Auftragnehmer werden sorgfältig ausgesucht.
☒ Klare und unzweifelhafte vertragliche Regelungen zur Datenverarbeitung
☒ Formalisiertes Weisungsmanagement
☒ Abschluss von Auftragsverarbeitungsverträgen.
☒ Kontrolle des Auftragnehmers durch die Geschäftsführung oder den Datenschutzbeauftragten
☒ Einsatz von EU-Standard-Vertragsklauseln (sofern erforderlich)
☐ …

Datenschutz-Management
Maßnahmen, die eine Steuerung der Datenschutzprozesse ermöglichen und die Einhaltung der datenschutzrechtlichen Vorgaben nachweisbar sicherstellen:

☒ Es wurde eine fachkundige Person zum Datenschutzbeauftragten benannt.
☒ Beschäftigte werden regelmäßig im Datenschutz geschult und sensibilisiert und sind über die Vertraulichkeit von Daten belehrt.
☒ regelmäßige Überprüfung der technischen und organisatorischen Maßnahmen
☒ Definierte Prozesse zur Erfüllung von Betroffenenrechte und Meldung von Datenpannen
☒ regelmäßige Überprüfung der technischen und organisatorischen Maßnahmen
☒ Definition von Aufbewahrungs- und Löschfristen

5. Pseudonymisierung (Art. 32 Abs. 1 lit. a) DSGVO, Art. 25 Abs. 1 DSGVO)
Maßnahmen, die gewährleisten, dass personenbezogene Daten in einer Weise verarbeitet werden, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

☒ Verwendung eines Proxy-Servers zur Weitergabe von Anfragen an KI-Tools in anonymisierter Form

Anlage 3: Unterauftragnehmer

Name	Anschrift/Land	Auftragsinhalt	Geeignete Garantien
DigitalOcean, LLC	101 Avenue of the Americas NY 10013 USA	Hosting	Zertifizierung nach dem U.S.-EU Privacy Framework (Angemessenheitsbeschluss) ISO 27001
PLUS FIVE FIVE, Inc.	2261 Market Street San Francisco CA 94114 USA	Transaktionale E-Mails	Zertifizierung nach dem U.S.-EU Privacy Framework (Angemessenheitsbeschluss) ISO 27001

Darüber hinaus sind auf der Plattform Inhalte von den nachstehenden Drittanbietern eingebunden. Bei der Einbindung dieser Inhalte schalten wir einen Proxy-Server dazwischen. Hierdurch wird die IP-Adresse des Nutzers der Plattform nicht an den Browser des Drittanbieters gesendet. Bei einer Nutzung gemäß unseren Nutzungsbedingungen werden somit keine personenbezogenen Daten an die Drittanbieter übermittelt. Eine Verarbeitung von personenbezogenen Daten erfolgt lediglich, wenn Nutzeranfragen personenbezogene Daten enthalten.

Name	Anschrift/Land	Auftragsinhalt	Geeignete Garantien
Mistral AI	15 rue des Halles 75001 Paris Frankreich	Hosting von Sprachmodellen via API	ISO 27001
Microsoft Deutschland GmbH	Walter-Gropius-Strasse 5 80807 München Deutschland	Hosting von Sprachmodellen via API, Bilderzeugung/-erkennung	ISO 27001
Anthropic Ireland, Ltd	6th Floor, South Bank House Barrow Street Dublin 4, D04 TR29 Ireland	Hosting von Sprachmodellen via API	ISO 27001