4 A-SIDE
PROF. DR. KAUFFELD & LORENZO

Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO

zwischen

den Kunden, die über testothek.online einen Vertrag geschlossen haben

- Verantwortlicher -

- nachstehend Auftraggeber genannt -

und

4A-SIDE GmbH
Spielmannstraße 19
38106 Braunschweig

- Auftragsverarbeiter -

- nachstehend Auftragnehmer genannt -

1. Vertragsgegenstand

Der Auftragsnehmer erhält Zugriff auf die personenbezogenen Daten des Auftraggebers, die im Rahmen der Nutzung der testothek.online Testplattform (im Folgenden Testplattform) durch den Auftraggeber erhoben werden. Außerdem kann im Rahmen der Erledigung von Supportanfragen des Auftraggebers bei dem Auftragnehmer nicht ausgeschlossen werden, dass der Auftragnehmer Zugriff auf personenbezogene Daten erhält bzw. von diesen Daten Kenntnis erlangt, für die der Auftraggeber verantwortliche Stelle oder selbst Auftragsverarbeiter im Sinne der datenschutzrechtlichen Vorschriften ist (nachfolgend „Auftraggeber-Daten“ genannt). Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang des Auftragnehmers mit Auftraggeber-Daten zur Erledigung der Supportanfragen.

2. Art, Umfang, Zweck und Laufzeit der Auftragsdatenverarbeitung

2.1. Der Auftragnehmer verarbeitet die Auftraggeber-Daten im Auftrag und nach Weisung des Auftraggebers (Auftragsdatenverarbeitung). Der Auftraggeber bleibt im datenschutzrechtlichen Sinn verantwortliche Stelle („Herr der Daten“).

2.2. Die Verarbeitung der Auftraggeber-Daten im Rahmen der Auftragsverarbeitung erfolgt in Umfang, Art und Zweck ausschließlich, um dem Auftraggeber die Funktionen der Testplattform

zur Verfügung zu stellen sowie ggfs. zur Erbringung von Supportleistungen. Die Verarbeitung umfasst die Registrierung der Daten der Nutzenden, um Zugang zur Testplattform zu erhalten sowie Daten der Teilnehmenden, um die Durchführung von Fragebögen zu ermöglichen.

2.3. Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen Nutzende der Testplattform sowie Teilnehmende, die Befragungen über die Testplattform ausfüllen.

2.4. Die Art der Daten umfassen folgende

a) Für Nutzende der Testplattform:

- Name
- E-Mail-Adresse
- Handynummer
- Ggf Adresse

b) Für Teilnehmende der Testplattform:

- Ggf. Name
- Ggf. E-Mail-Adresse
- Ggf. Teilnehmenden-Code
- Daten beim Ausfüllen des Fragebogens

2.5. Die Verarbeitung der Auftraggeber-Daten findet ausschließlich im Gebiet der Europäischen Union statt.

2.6. Die Laufzeit und Kündigung dieses Vertrags richtet sich nach den Bestimmungen zur Laufzeit und Kündigung des von dem Auftragnehmer über testothek.online erteilten Auftrags zur Nutzung der Testplattform. Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen.

3. Weisungsbefugnisse des Auftraggebers; Berichtigung, Einschränkung und Löschung von Daten

3.1. Der Auftragnehmer darf die Auftraggeber-Daten nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

3.2. Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

3.3. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

4. Pflichten des Auftragnehmers

4.1. Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Auftraggeber-Daten vor der unbefugten Kenntnisnahme Dritter geschützt sind. Insbesondere gewährt der Auftragnehmer die Einhaltung folgender Vorgaben:

- Schriftliche Bestellung eines Datenschutzbeauftragten nach den gesetzlichen Vorschriften. Als Datenschutzbeauftragter ist beim Auftragnehmer Herr Hendrik Sievers, beck Service GmbH, Ericusspitze 4, 20457 Hamburg, Telefon: 040 / 3010070, E-Mail: datenschutz@4a-side.com, bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.
- Die Wahrung der Vertraulichkeit. Der Auftragnehmer setzt bei der Durchführung nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet sind und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden.
- Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen (Einzelheiten in der **Anlage 1**).
- Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
- Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
- Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
- Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

5. Unterauftragsverhältnisse

5.1. Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Auftraggeber-Daten auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

5.2. Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen. Der Auftraggeber stimmt der Beauftragung der in **Anlage 2** bezeichneten Unterauftragnehmer

unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO mit dem Unterauftragnehmer zu. Die vertragliche Vereinbarung wird dem Auftraggeber auf dessen Verlangen vorgelegt, wobei geschäftliche Klauseln ohne datenschutzrechtlichen Bezug hiervon ausgenommen sind.

6. Technische und organisatorische Maßnahmen

6.1. Der Auftragnehmer hat vor Beginn der Verarbeitung der Auftraggeber-Daten die in der **Anlage 2** dieses Vertrags aufgelisteten technischen und organisatorischen Maßnahmen zu implementieren und während des Vertrags aufrechtzuerhalten.

6.2. 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 der **Anlage 2** festgelegten Maßnahmen nicht unterschritten wird. Der Auftragnehmer wird solche Änderungen dokumentieren. Wesentliche Änderungen der Maßnahmen bedürfen der vorherigen schriftlichen Zustimmung des Auftraggebers und sind vom Auftragnehmer zu dokumentieren und dem Auftraggeber auf Anforderung zur Verfügung zu stellen.

7. Kontrollrechte des Auftraggebers

7.1. Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

7.2. Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

7.3. Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit.

8. Mitteilung bei Verstößen des Auftragnehmers

8.1. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der gesetzlichen Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

- die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung

durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen;

- die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden;
- die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen;
- die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung;
- die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

8.2. Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

8.3. Für den Fall, dass eine betroffene Person ihre Rechte auf Berichtigung, Löschung oder Sperrung von Auftraggeber-Daten oder auf Auskunft über die gespeicherten Auftraggeber-Daten, den Zweck der Speicherung und die Personen und Orte, an die Auftraggeber-Daten regelmäßig übermittelt werden, geltend macht, hat der Auftragnehmer den Auftraggeber bei der Erfüllung dieser Ansprüche in angemessenem und für den Auftraggeber erforderlichen Umfang zu unterstützen, sofern der Auftraggeber die Ansprüche nicht ohne Mitwirkung des Auftragnehmers erfüllen kann.

8.4. Der Auftragnehmer wird es dem Auftraggeber ermöglichen, Auftraggeber-Daten zu berichtigen, zu löschen oder zu sperren oder auf Verlangen des Auftraggebers die Berichtigung, Sperrung oder Löschung selbst vornehmen, wenn und soweit das dem Auftraggeber selbst unmöglich ist.

9. Rückgabe und Löschung überlassener Daten und Datenträger

9.1. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

9.2. Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

9.3. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

4A-SIDE GmbH

Anlagen:
Anlage 1: Technische und organisatorische Maßnahmen
Anlage 2: Unterauftragnehmer

4 A-SIDE
PROF. DR. KAUFFELD & LORENZO

Anlage 1:
Beschreibung der technischen und organisatorischen Maßnahmen zum Datenschutz gemäß Art. 32 DS-GVO der 4-A-Side GmbH

1. Vertraulichkeit:

Zutrittskontrolle:

☒ Zutrittskontrolle durch Transponder-Schließsystem, Schlüsselregelung
☒ Aufenthalt von Besuchern nur in Anwesenheit von Mitarbeitern
☒ Videoüberwachung am Serverraum
☒ Fenster einbruchsicher (4. Stock)
☒ Serverraum verschlossen, Zutritt nur für EDV-Mitarbeiter, Geschäftsführung
☒ Sorgfältige Auswahl Reinigungspersonal

Zugangskontrolle:

☒ Identifizierung und Authentifizierung durch Benutzername/Passwort
☒ Passwortrichtlinie
- Minimale Kennwortlänge: 8 Zeichen
- Komplexität: „4 aus 4“ (Großbuchstaben, Kleinbuchstaben, Zahlen, Sonderzeichen)
- Keine Weitergabe von Passwörtern

☒ Begrenzung der Fehlversuche
☒ Systemverwalterbefugnisse/ -protokollierung
☒ Arbeitsanweisung Sperren des Bildschirms bzw. Abmelden vom System
☒ Protokollierung der Anmeldung
☒ Firewalls (2x) und Antivirensoftware

Zugriffskontrolle:

☒ Berechtigungskonzept mit Rollen und unterschiedlichen Berechtigungsstufen
☒ Definierte VPN-Benutzerprofile gem. Benutzertätigkeiten für den Zugriff von extern auf die IT-Systeme
☒ Administratoren-Rechte auf das „Notwendigste“ reduziert
☒ Datenträgervernichtung intern mit Protokollierung
☒ Vernichtung Papier intern mit Aktenvernichter, Sicherheitsstufe 4 (geheimzuhaltendes Schriftgut)
☒ Verschlüsselung von Datenbanken und Datenträgern

Trennungsgebot:

☒ Projektbezogen jeweils getrennte virtuelle Entwicklungs-, Demo- und Livesysteme zum Verarbeiten von Daten
☒ Logische Kundentrennung (softwareseitig)
☒ Unterschiedliche Datenbanken
☒ Festlegung von Datenbankrechten
☒ Physikalische Trennung Personaldaten (Papierakten), logische Trennung digitaler Personaldaten über Berechtigungskonzept

2. Integrität:

Weitergabekontrolle:

☒ Bestandsverzeichnis und Bestandskontrolle der Datenträger durch mit Leitung der Datenverarbeitung beauftragte Person und den Datenschutzbeauftragten
☒ Es erfolgt keine Weitergabe von Datenträgern an Dritte
☒ Einsatz VPN-Technologie
☒ Sichere Aufbewahrung von Datenträgern

Eingabekontrolle:

☒ Protokollierung der Eingabe, Änderung und Löschung von Daten auf relevanten Datenbank-Feldern
☒ Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können
☒ Rechtevergabe Lesen, Eingeben, Änderung und Löschung im Rahmen des Berechtigungskonzeptes

3. Verfügbarkeit und Belastbarkeit:

Verfügbarkeitskontrolle:

☒ Serverraum nicht unter sanitärer Anlage
☒ Klimaanlage im Serverraum
☒ Schutzsteckdosenleisten im Serverraum
☒ Unterbrechungsfreie Stromversorgung (USV)
☒ Angriff von außen: Firewall (2x)
☒ Risiko- und Schwachstellenanalyse im Rahmen des jährlichen Audits durch den Datenschutzbeauftragten
☒ alle 24h ein Backup in einen sicheren, ausgelagerten Ort (Datentresor)
☒ Testen von Datenwiederherstellung
☒ Schulung der Mitarbeiter bezüglich Sicherheitsanforderungen durch den Datenschutzbeauftragten

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung:

Datenschutzmanagement:

☒ Dokumentation Verfahren / Verfahrensregister sind vorhanden, vollständig und aktuell
☒ Fachkundenachweise des Datenschutzbeauftragten liegen vor
☒ Einhaltung Datengeheimnis, sämtliche Mitarbeiter sind auf das Datengeheimnis verpflichtet
☒ Regelmäßige Datenschutzmerkblätter für die Mitarbeiter, Datenschutzschulung durch den Datenschutzbeauftragten
☒ Dienstanweisung über die Internet- und E-Mail-Nutzung
☒ jährliche Audits durch den Datenschutzbeauftragten

Incident-Response-Management:

☒ Etwaige Vorfälle werden unverzüglich dem Datenschutzbeauftragten gemeldet
☒ Bearbeitung etwaiger Fälle durch den Datenschutzbeauftragten

Auftragskontrolle:

☒ Schriftliche Verträge zur Auftragsdatenverarbeitung liegen vor und werden jährlich auditiert durch den Datenschutzbeauftragten
☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
☒ Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
☒ Kontrolle der Einhaltung beim Auftragnehmer und/oder Überprüfung Zertifikat(e) durch den Datenschutzbeauftragten, Protokollierung

Technische und organisatorische Maßnahmen in dem Rechenzentrum

(Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen)

Die Darstellung der technischen und organisatorischen Maßnahmen beschränkt sich für die Dienstleistungen in dem Rechenzentrum auf die Beschreibung der Zutrittskontrollen und der Verfügbarkeitskontrollen. Dies erfolgt im Einklang mit den Empfehlungen der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) gem. GDD-Ratgeber Datenschutz-Prüfung von Rechenzentren:

Zutrittskontrolle:

- Datacenterparks in Nürnberg und Falkenstein
  - elektronisches Zutrittskontrollsystem mit Protokollierung
  - Hochsicherheitszaun um den gesamten Datacenterpark
  - dokumentierte Schlüsselvergabe an Mitarbeiter und Colocation-Kunden für Colocation Racks (jeder Auftraggeber ausschließlich für seinen Colocation Rack)
  - Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
  - 24/7 personelle Besetzung der Rechenzentren
  - Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen
  - Der Zutritt für betriebsfremde Personen (z.B. Besucherinnen und Besucher) zu den Räumen ist wie folgt beschränkt: nur in Begleitung eines Hetzner Online GmbH Mitarbeiters
- Verwaltung
  - elektronisches Zutrittskontrollsystem mit Protokollierung
  - Videoüberwachung an den Ein- und Ausgängen

Verfügbarkeitskontrolle

- Backup- und Recovery-Konzept mit täglicher Sicherung der Daten je nach gebuchten Leistungen des Hauptauftrages.
- Einsatz von Festplattenspiegelung.
- Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
- Einsatz von Softwarefirewall und Portreglementierungen.
- Dauerhaft aktiver DDoS-Schutz.

Für alle internen Systeme ist eine Eskalationskette definiert, die vorgibt wer im Fehlerfall zu informieren ist, um das System schnellstmöglich wiederherzustellen.

Anlage 2:
Unterauftragnehmer

Unternehmen:	**Leistungen:**
Hetzner Online GmbH Industriestr. 25 91710 Gunzenhausen Deutschland	Betrieb des zertifizierten Rechenzentrums, aus dem die Testplattform betrieben wird.
4A-SIDE Iberica Avenida Tio Pepe 8 11407 Jerez de la Frontera	IT Umsetzung und Support der Plattform