Auftragsverarbeitungsvertrag

Kunde

nachstehend **“Verantwortlicher”** genannt

und

MeisterLabs GmbH
Zugspitzstraße 2
85591 Vaterstetten
Germany

nachstehend “Auftragsverarbeiter” genannt

einzeln als **“Partei”**, gemeinsam als **“Parteien”** bezeichnet

schließen den folgenden Auftragsverarbeitungsvertrag (**“AVV”**) über die Datenverarbeitung zur Regelung der Verarbeitung personenbezogener Daten ab.

1 Präambel

1.1 Dieser AVV bildet einen Anhang zu den Allgemeinen Geschäftsbedingungen (“AGB”), die auch für diesen AVV gelten, sofern in diesem AVV nicht anders angegeben wird.

1.2 Mit der Annahme der AGB haben der Verantwortliche und der Auftragsverarbeiter diesen AVV als Teil der Click-through-Vereinbarung akzeptiert, um sicherzustellen, dass die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen in Übereinstimmung mit den geltenden Datenschutzgesetzen erfolgt.

2 Definitionen

2.1 “Datenschutzgesetze” umfassen die Allgemeine Datenschutzgrundverordnung der EU (EU/2016/679) (“**DSGVO**”) sowie alle nationalen Datenschutzgesetze und -bestimmungen, die die Datenverarbeitungstätigkeiten im Rahmen dieses AVV regeln.

2.2 “Personenbezogene Kundendaten” umfassen alle personenbezogenen Daten, die der Auftragsverarbeiter und etwaige von ihm eingesetzte Unterauftragsverarbeiter im Auftrag des Verantwortlichen gemäß dieses AVV verarbeiten.

2.3 Alle in diesem AVV verwendeten Begriffe sind im Sinne der EU-DSGVO, sofern nicht ausdrücklich etwas anderes vereinbart wurde.

3 Rechte und Pflichten des Verantwortlichen

3.1 Der Verantwortliche verpflichtet sich, die Personenbezogenen Kundendaten, die dem Auftragsverarbeiter und entwaigen Unterauftragsverarbeitern übermittelt wurden, in Übereinstimmung mit den einschlägigen und anwendbaren Gesetzen und Vorschriften zu verarbeiten. Es liegt in der alleinigen Verantwortung Verantwortlichen, erforderliche Einwilligungen einzuholen und die Rechtmäßigkeit der Verarbeitung Personenbezogener Kundendaten sicherzustellen.

4 Rechte und Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter ist verpflichtet

4.1 Personenbezogene Kundendaten nur entsprechend der dokumentierten Anweisung des Verantwortlichen, den AGB und seinen gesetzlichen Verpflichtungen zu verarbeiten. Die Anweisungen für alle zur Vertragserfüllung notwendigen Verarbeitungsschritte gelten mit Vertragsabschluss als erteilt.

4.2 den Verantwortlichen unverzüglich zu benachrichtigen, wenn der Auftragsverarbeiter der Ansicht ist, dass die Anweisungen des Verantwortlichen gegen die geltenden Datenschutzgesetze verstoßen. Daraus ergibt sich jedoch keine Verpflichtung für den Auftragsverarbeiter, Rechtsberatung einzuholen. Ebenso wenig stellt die Erfüllung dieser Verpflichtung eine Rechtsberatung für den Verantwortlichen dar.

4.3 soweit dies möglich ist, den Verantwortlichen unverzüglich über alle Anfragen, Beschwerden, Meldungen, Anträge oder sonstigen Mitteilungen (im Folgenden als “Antrag” bezeichnet) zu informieren, die von einer Aufsichts- oder Regierungsbehörde oder einem sonstigen Dritten in Bezug auf die Verarbeitung Personenbezogener Kundendaten durch den Auftragsverarbeiter eingehen. Der Auftragsverarbeiter wird den Verantwortlichen auf dessen Anfrage in angemessener Weise unterstützen, auf einen solchen Antrag in Übereinstimmung mit den geltenden Datenschutzgesetzen zu antworten. Die Beantwortung erfolgt ausschließlich durch den Verantwortlichen, es sei denn, der Auftragsverarbeiter ist nach zwingendem Recht verpflichtet, direkt zu antworten.

4.4 den Verantwortlichen angesichts der Art der Verarbeitung dabei zu unterstützen, seiner Verpflichtung zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO (EU/2016/679) genannten Rechte (zB Auskunft, Information, Berichtigung und Löschung, Datenübertragbarkeitl) in Bezug auf die Verarbeitung Personenbezogener Kundendaten nachzukommen.

4.5 den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Art. 32 bis 36 der DSGVO genannten Pflichten (zB Datensicherheitsmaßnahmen, Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde und an die betroffenen Personen,

Datenschutz-Folgenabschätzung, Konsultation de Aufsichtsbehörde) in Bezug auf die Verarbeitung Personenbezogener Kundendaten zu unterstützen, und zwar insbesondere

a) den Verantwortlichen so bald wie möglich zu benachrichtigen, wenn der Auftragsverarbeiter Kenntnis von einer Verletzung des Schutzes personenbezogener Daten erhält, die unmittelbaren Einfluss auf Personenbezogenen Kundendaten ("Datenschutzvorfall") erhält;

b) sich angemessen zu bemühen, dem Verantwortlichen so bald wie möglich vernünftigerweise erforderliche Informationen über den Datenschutzvorfall zu übermitteln.

4.6 alle Personenbezogenen Kundendaten auf schriftliche Anfrage und Beendigung des Hauptvertrags, unabhängig von den Gründen für die Beendigung, gemäß dieses AVV zu löschen. Wenn gesetzliche Verpflichtungen, an die der Auftragsverarbeiter gebunden ist, dies erfordern, kann der Auftragsverarbeiter im Einklang mit diesen Verpflichtungen eine Kopie der Daten des Verantwortlichen aufbewahren. Darüber hinaus ist der Auftragsverarbeiter berechtigt, alle erforderlichen Aufzeichnungen und Informationen (zu denen auch Personenbezogenen Kundendaten gehören können), aufzubewahren, die er benötigt, um die Einhaltung seiner Verpflichtungen aus dem Hauptvertrag und dieses AVV unter Einhaltung der geltenden gesetzlichen Verjährungsfristen nachzuweisen.

4.7 Der Auftragsverarbeiter wird dem Verantwortlichen auf Anfrage alle Informationen zur Verfügung stellen, die erforderlich sind, um die Einhaltung der in diesem AVV, dem Hauptvertrag oder den Datenschutzgesetzen festgelegten Pflichten nachzuweisen.

5 Unterauftragsverarbeiter

5.1 Der Verantwortliche erteilt hiermit seine allgemeine Zustimmung zur Beauftragung von Unterauftragsverarbeiter im Zusammenhang mit der Verarbeitung von Personenbezogenen Kundendaten unter diesem AVV.

5.2 Der Auftragsverarbeiter verpflichtet sich, den Verantwortlichen über jede Änderung hinsichtlich der Einschaltung oder Ersetzung weiterer Unterauftragsverarbeiter zu informieren. Sofern der Verantwortliche nicht innerhalb von vierzehn (14) Tagen schriftlich unter Angabe von vernünftigen datenschutzrechtlichen Gründen widerspricht, gilt die Einschaltung oder Ersetzung als genehmigt. Widerspricht der Verantwortliche rechtzeitig und wirksam, so bemüht sich der Auftragsverarbeiter im Rahmen des wirtschaftlich Zumutbaren, die betreffenden Leistungen für den Verantwortlichen zu erbringen, ohne den widersprochenden Unterauftragsverarbeiter mit der Verarbeitung der personenbezogenen Daten des Kunden zu beauftragen. Ist dies wirtschaftlich nicht zumutbar und ist der Wechsel des Unterauftragsverarbeiters für den Verantwortlichen aus den genannten Gründen unzumutbar, kann der Verantwortliche die Vereinbarung mit einer Frist von vierzehn (14) Tagen durch schriftliche Mitteilung an den Unterauftragsverarbeiter kündigen. Die Widerspruchs- und Kündigungsrechte nach dieser Ziffer 5.2 gelten nicht, wenn der betreffende Auftragsverarbeiter ausschließlich im Zusammenhang mit optionalen Funktionen oder Features des Services eingesetzt wird, deren Verwendung dem Verantwortlichen frei steht.

5.3 Soweit der Auftragsverarbeiter Unterauftragsverarbeiter in die Leistungserfüllung einbezieht, ist er verpflichtet

a) durch eine schriftliche Vereinbarung sicherzustellen, dass alle Unterauftragsverarbeiter im Wesentlichen an die gleichen Verpflichtungen gebunden sind, die für den Auftragsverarbeiter gemäß dieses AVV gelten.

b) die Haftung gegenüber dem Verantwortlichen zu übernehmen, wenn ein Unterauftragsverarbeiter seinen Datenschutzverpflichtungen aus der schriftlichen Vereinbarung im Sinne von Abschnitt a) nicht nachkommt.

6 Internationale Datenübertragungen

6.1 Der Auftragsverarbeiter kann personenbezogene Daten innerhalb des Europäischen Wirtschaftsraums ("EWR") oder in Ländern verarbeiten, die nach Auffassung der Europäischen Kommission ein angemessenes Schutzniveau gewährleisten ("Angemessene Drittländer").

6.2 Der Auftragsverarbeiter darf Personenbezogene Kundendaten an Unterauftragsverarbeiter, die in Ländern ansässig sind, die nach Ansicht der Europäischen Kommission kein angemessenes Datenschutzniveau gewährleisten, übermitteln, soweit der Auftragsverarbeiter sicherstellt, dass die in Kapitel V der DSGVO genannten Anforderungen eingehalten werden. Der Auftragsverarbeiter gewährleistet die Einhaltung der Vorschriften durch die Einführung geeigneter Garantien für die Übermittlung gemäß Kapitel V der Datenschutz-Grundverordnung.

6.3 Wenn eine Schutzmaßnahme, auf die sich der Auftragsverarbeiter für die rechtmäßige Übermittlung Personenbezogener Kundendaten stützt, nicht mehr gültig ist oder anderweitig nicht ausreicht, um die Einhaltung von Kapitel V der DSGVO zu gewährleisten, unternimmt der Auftragsverarbeiter wirtschaftlich vertretbare Anstrengungen, um eine andere gültige Schutzmaßnahme einzuführen oder andere geeignete Maßnahmen zu ergreifen, um die Rechtmäßigkeit der Übermittlungen weiterhin zu gewährleisten.

7 Technische und Organisatorische Maßnahmen

7.1 Der Auftragsverarbeiter verpflichtet sich, die erforderlichen technischen und organisatorischen Maßnahmen zu ergreifen, um die Einhaltung der geltenden Datenschutzgesetze in diesem AVV zu gewährleisten. Eine Übersicht über die vom Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen ist in Anhang 2 enthalten. Der Verantwortliche bestätigt, dass die in Anhang 2 angeführten technischen und organisatorischen Maßnahmen angemessen sind.

7.2 Der Auftragsverarbeiter ist verpflichtet, dem Verantwortlichen alle wesentlichen Änderungen der technischen oder organisatorischen Maßnahmen mitzuteilen, sofern eine solche Änderung nicht zu einer verbesserten Gesamtsicherheit der vom Datenverarbeiter erbrachten Dienstleistungen führt.

8 Audit

8.1 Der Verantwortliche erkennt an und erklärt sich damit einverstanden, dass der Auftragsverarbeiter die Einhaltung seiner Verpflichtungen gemäß dieses AVV nachweisen kann, indem er eine geeignete Dokumentation seiner Sicherheitsmaßnahmen und einschlägigen aktuellen Zertifizierungen („Compliance-Dokumentation") zur Verfügung stellt. Eine solche Compliance-Dokumentation ist auf angemessene Anfrage des Verantwortlichen vorzulegen und wird in der Regel als ausreichend erachtet, um die Einhaltung der Verpflichtungen des Datenverarbeiters zu überprüfen.

8.2 Sofern die Compliance-Dokumentation nach vernünftigem Ermessen des Verantwortlichen nicht ausreicht, um die Einhaltung einer bestimmten Pflicht gemäß dieses AVV zu überprüfen, und (i) der Verantwortliche dokumentierte Nachweise vorlegt, die einen begründeten Verdacht auf einen

erheblichen Verstoß des Auftragsverarbeiters gegen seine Pflichten gemäß dieses AVV in Bezug auf diese bestimmte Pflicht begründen; oder (ii) eine Prüfung von der zuständigen Aufsichtsbehörde des Verantwortlichen gemäß anwendbaren Datenschutzrechts ausdrücklich verlangt wird, gestattet der Auftragsverarbeiter dem Verantwortlichen oder einem vom Verantwortlichen beauftragten und vom Auftragsverarbeiter genehmigten unabhängigen Prüfer die Durchführung einer Prüfung vor Ort (Audit"), gemäß dem in Ziffer 8.3 beschriebenen Verfahren.

8.3 Für jedes nach Abschnitt 8.2 zulässige Audit gilt Folgendes

(a) Der Umfang des Audits ist strikt auf die Überprüfung der Einhaltung der spezifischen Verpflichtungen beschränkt, die zu den in Klausel 8.2 festgelegten Anforderungen führen.

(b) Das Audit wird nach schriftlicher Ankündigung mit einer Frist von mindestens 30 Tagen und während der üblichen Geschäftszeiten des Datenverarbeiters durchgeführt und ist so zu organisieren, dass der Betrieb des Datenverarbeiters so wenig wie möglich beeinträchtigt wird.

(c) Bei dem Prüfer muss es sich um einen unabhängigen Dritten handeln, der kein Wettbewerber des Auftragsverarbeiters ist, für den Auftragsverarbeiter nach vernünftigem Ermessen annehmbar ist und einer angemessenen Geheimhaltungspflicht unterliegt.

(d) Der Verantwortliche trägt alle mit dem Audit verbundenen Kosten, einschließlich der angemessenen Kosten des Auftragsverarbeiters für die Unterstützung des Audits.

9 Vertraulichkeit der Daten

Der Auftragsverarbeiter gewährleistet, dass die von ihm mit der Verarbeitung der Personenbezogenen Kundendaten beauftragten Personen sich zur Vertraulichkeit verpflichtet haben oder gesetzlich zur Geheimhaltung verpflichtet sind.

10 Laufzeit und Kündigung

10.1 Dieser AVV tritt gemäß Punkt 1.2. in Kraft und gilt so lange, wie der Auftragsverarbeiter im Auftrag des Verantwortlichen personenbezogene Daten im Zusammenhang mit der Erbringung von Dienstleistungen im Rahmen des Hauptvertrags verarbeitet.

11 Allgemeine Bestimmungen

11.1 Änderungen dieses AVV unterliegen den in den AGB festgelegten Voraussetzungen.

11.2 Sollten der Verantwortliche und der Auftragsverarbeiter zusätzliche Vereinbarungen treffen, die im Widerspruch zu diesem AVV stehen, haben die Bestimmungen dieses AVV, die sich auf die Verarbeitung Personenbezogener Kundendaten beziehen, vor allen entgegenstehenden Bestimmungen Vorrang.

Meister

Anhang 1

Wenn der Verantwortliche den Auftragsverarbeiter mit der Verarbeitung zusätzlicher personenbezogener Daten beauftragen möchte, die über die nachstehend genannten personenbezogenen Daten hinausgehen, muss er dies dem Auftragsverarbeiter mitteilen. Der Auftragsverarbeiter wird den Antrag prüfen und – wenn möglich – die Änderungen bestätigen.

Datensubjekte

Die verarbeiteten personenbezogenen Daten sind abhängig von den vom Verantwortlichen zur Verfügung gestellten personenbezogenen Daten und können sich auf die folgenden Kategorien von Datensubjekten beziehen:

- Kunden des Verantwortlichen
- Kunden von Kunden des Verantwortlichen
- Mitarbeiter des Verantwortlichen
- Mitarbeiter von Kunden des Verantwortlichen
- Ansprechpartner von Lieferanten des Verantwortlichen
- Ansprechpartner von Lieferanten von Kunden des Verantwortlichen
- Interessenten des Verantwortlichen
- Interessenten von Kunden des Verantwortlichen

Datenkategorien

Die verarbeiteten Datenkategorien hängen von den vom Verantwortlichen zur Verfügung gestellten personenbezogen Daten ab und können folgende Datenkategorien beinhalten:

- Personalstammdaten (zB Anrede, Nachname, Vorname, Anschrift, Titel, Beruf)
- Kommunikationsdaten (Kommunikationsinhalte)
- Planungs- und Steuerungsdaten
- Daten, die Nutzer in Nachrichten, Freitextfeldern oder als Inhalt von Dateien von sich aus übermitteln: Freitextfeld-Eingaben im Rahmen der Erstellung von Mindmaps durch Benutzer, Freitextfeld-Eingaben im Rahmen der Planung von Tasks durch Benutzer, Dateien und Bilder, die im Rahmen der Erstellung von MindMaps und Tasks durch den Benutzer hochgeladen werden

Besondere Datenkategorien

Nein.

Umfang, Art und Zweck der Datenverarbeitung, Art der personenbezogenen Daten und Datensubjekte

Der Auftragsverarbeiter bietet ein Online-Mindmapping-Tool an, mit dem Ideen visualisiert, entwickelt und geteilt werden können. Der Mindmap-Editor wird für das Brainstorming, die Strukturierung von Informationen, die Erstellung von Notizen und die Planung von Projekten beim Verantwortlichen verwendet.

Der Auftragsverarbeiter bietet ein Task-Management-Tool an, mit dem der Verantwortliche Projekte erstellen und Aufgaben an verschiedene Teammitglieder vergeben kann. Der Verantwortliche kann zudem Checklisten und Fristen in den Aufgaben verwalten, den Projektfortschritt einsehen und verfolgen.

Der Auftragsverarbeiter bietet ein Online-Dokumentation-Tool an, mit dem vom Verantwortlichen Notizen und Dokumente erstellt und mit Teammitgliedern geteilt werden können. Die Dokumente werden für Notizen, Checklisten, Präsentationen und die Weitergabe von Informationen an Mitarbeiter verwendet.

Personenbezogene Kundendaten werden im Rahmen des AVV zum Zweck der Erbringung der Leistungen und zur Erfüllung der Verpflichtungen des Auftragsverarbeiters gemäß geltendem Recht, dem Hauptvertrag und diesem AVV verarbeitet.

Die Art der Verarbeitung hängt von der Nutzung des Dienstes durch den Verantwortlichen ab und kann je nach Nutzung des Dienstes durch den Verantwortlichen das Speichern, Ändern, Anzeigen, Strukturieren, Organisieren und Kombinieren umfassen.

Meister

Anhang 2 - Überblick über technische und organisatorische Maßnahmen

Der Auftragsverarbeiter kann diese technischen und organisatorischen Maßnahmen jederzeit aktualisieren, vorausgesetzt, dass eine solche Aktualisierung die Sicherheit der vom Auftragsverarbeiter erbrachten Leistungen insgesamt nicht vermindert.

Datenschutz / Sicherheitskonzept

Die Datenschutzrichtlinien des Verantwortlichen und des Auftragsverarbeiters (einschließlich aller einschlägigen Sicherheitsrichtlinien) betreffen die Sicherheit personenbezogener Daten.

Organisatorische Sicherheitsmaßnahmen

Die interne Organisation ist so gestaltet, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

- Es gelten Richtlinien und Verfahren, welche regelmäßig geprüft werden.
- Risiken werden bewertet und dokumentiert.
- Informationen werden gemäß einer Richtlinie klassifiziert.
- Es wurde ein Security Manager ernannt.
- Geeignete Messungen der Leistung und Wirksamkeit des Sicherheitsmanagement werden durchgeführt.

Sicherheitsmaßnahmen bei Änderung eines Dienstes

Der Änderungsmanagement-Prozess umfasst eine Analyse der Auswirkungen auf den Datenschutz und eine Bewertung der Informationssicherheitsrisiken.

Personenbezogene Daten dürfen für die Prozess- oder Systementwicklung und die damit verbundenen Tests nur dann verwendet werden, wenn sie vor ihrer Verwendung anonymisiert oder anderweitig geschützt wurden.

Sicherheitsmaßnahmen in der Benutzerverwaltung

Maßnahmen verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- Passwörter werden mit einem Passwort Manager verwaltet.
- Es gibt eine Passwortrichtlinie, die durch den Passwort Manager und ein System zur Verwaltung mobiler Geräte verstärkt wird.
- Die Zwei-Faktor-Authentifizierung wird dort durchgeführt, wo es unsere Richtlinie verlangt.

Sicherheitsmaßnahmen für den logischen Zugriff

Der logische Zugriff auf personenbezogene Daten ist eingeschränkt. Maßnahmen stellen sicher, dass die zur Nutzung der Datenverarbeitungssysteme berechtigten Personen nur auf die Daten zugreifen können, für die sie berechtigt sind.

- Der Zugriff wird nach dem Need-to-know-Prinzip (Erforderlichkeitsprinzip) gewährt.
- Der Zugriff wird auf Antrag gewährt/widerrufen. Der Widerruf kann auch automatisch nach einer bestimmten Zeitspanne oder manuell nach einer Überprüfung erfolgen.
- Wir verfügen über ein Verfahren zur Beantragung von Genehmigungen, in dem der Benutzer, der Zugang benötigt, das System, die geforderten Genehmigungen, der Antragsteller und der Bevollmächtigte dokumentiert sind.
- Im Rahmen des HR-Onboarding- und des HR-Offboarding-Prozesses werden auch Zugriffsrechte gewährt/entzogen.
- Wir führen regelmäßige Überprüfungen des logischen Zugriffs auf alle unsere Systeme durch, abhängig von der Klassifizierung der Informationen, und dokumentieren diese Überprüfungen.

Aufteilung der Mandate

Die Kundendaten sind logisch aufgeteilt und durch Sicherheitsmechanismen voneinander getrennt. Darüber hinaus gibt es Test- und Staging-Systeme, die vollständig vom Produktivsystem getrennt sind.

Sicherheitsmaßnahmen für den physischen Zugang

Der physische Zugang zu personenbezogenen Daten in jedem Format ist begrenzt.

Personenbezogene Daten in jeglichem Format sind gegen versehentliche Offenlegung aufgrund von Naturkatastrophen und Umweltgefahren geschützt.

Personenbezogene Daten auf tragbaren Medien oder Geräten sind vor unbefugtem Zugriff geschützt. Sicherheitsmaßnahmen für Speichermedien verhindern unbefugtes Lesen, Kopieren, Ändern oder Entfernen von Speichermedien.

Google-Rechenzentrum (Frankfurt, Deutschland)

- Verschlüsselungsmaßnahmen und Zertifikate des Rechenzentrums:
  https://cloud.google.com/docs/security/encryption/default-encryption
  https://cloud.google.com/security/compliance/iso-27001/

MeisterLabs GmbH Büro (München, Deutschland)

- MeisterLabs GmbH Büro in München, Zugspitzstraße 2, 85591 Vaterstetten.
- Der Zugang zum Bürogebäude ist durch eine Außentür mit Schloss gesichert.
- Der Zugang zu den Büroräumen der MeisterLabs GmbH ist zusätzlich mit einem Schloss gesichert und nur mit den entsprechenden Schlüsseln möglich, die nur Mitarbeitern der MeisterLabs GmbH zur Verfügung stehen. Der Vermieter verfügt über keinen Schlüssel zu diesen Räumlichkeiten. Die Schlüssel werden den Mitarbeitern der MeisterLabs GmbH bei Vertragsabschluss ausgehändigt, bei Beendigung des Arbeitsverhältnisses wird der Schlüssel eingezogen. Zudem gibt es eine entsprechende Dokumentation über die im Umlauf befindlichen Schlüssel.
- Gäste oder Besucher werden im Büro der MeisterLabs GmbH nicht empfangen.
- Das Firmennetzwerk in den oben genannten Räumlichkeiten der MeisterLabs GmbH in München ist durch eine moderne Firewall geschützt.

Sicherheitsmaßnahmen für die Speicherung von Daten

Es gibt Maßnahmen, die eine unbefugte Eingabe sowie eine unbefugte Auswertung, Veränderung oder Löschung von gespeicherten personenbezogenen Daten verhindern. Dazu gehört auch der Schutz vor Schadsoftware.

- Cloud-Speicher

    - Die Daten werden auf Block-Ebene verschlüsselt, siehe “Sicherheitsmaßnahmen für den physischen Zugang”.
    - Der Zugang zu personenbezogenen Daten wird sorgfältig verwaltet, siehe “Sicherheitsmaßnahmen für den logischen Zugang”.
    - Die Computerressourcen in der Cloud werden automatisch auf Schwachstellen überprüft.
    - Ein Host Intrusion Detection System (HIDS) ist vorhanden, um ungewöhnliches Verhalten auf den Rechnern zu erkennen.
    - Tägliche Backups werden 14 Tage lang aufbewahrt, danach werden sie gelöscht.
- Mitarbeitergeräte
    - Alle Mitarbeitergeräte sind vollständig verschlüsselt. Eine Firewall und ein Virenschutz sind vorhanden. Automatische Bildschirmsperren sind aktiviert. Asset-Management-Prozesse sind implementiert. Alle Geräte sind in einer Mobile Device Management-Lösung registriert, um Richtlinien automatisch durchzusetzen.
    - Gestohlene oder verlorene Geräte können aus der Ferne gesperrt oder gelöscht werden.
    - Nur zugelassene Reparaturgeschäfte dürfen firmeneigene Geräte reparieren. Computer werden nur bei autorisierten Händlern gekauft.
    - Von der Speicherung von Daten auf Wechseldatenträgern wird abgeraten. Es gibt Richtlinien für die Entsorgung.

Sichere Entwicklungen

Es gilt die Secure Development Policy, um sicherzustellen, dass kein unsicherer Code eingeführt wird. Bestehende Codes und Bibliotheken von Drittanbietern werden regelmäßig auf Schwachstellen überprüft.

- Es gibt Maßnahmen zur Erkennung von unsicherem Code (statische Codeanalyse).
- Bei der Entwicklung muss unsere Secure Development Policy beachtet werden.
- Der gesamte Anwendungscode wird einer Peer Review unterzogen.
- Verwendete Bibliotheken werden automatisch auf bekannte Schwachstellen gescannt.

Sicherheitsmaßnahmen für die Dateneingabe

Es wird sichergestellt, dass überprüft werden kann, welche personenbezogenen Daten von wem und wann in die Datenverarbeitungssysteme eingegeben wurden.

Kontrolle der verarbeiteten Informationen

Das Datensubjekt hat die Möglichkeit, Auskunft über die Verarbeitung ihrer personenbezogenen Daten zu erhalten, sowie diese Daten berichtigen und löschen zu lassen.

Die Daten werden online direkt in der Datenbank oder im Onlinespeicher gelöscht und verschwinden nach 2 Wochen aus den Backups, sobald diese erneuert wurden.

Sicherheitsmaßnahmen bei der Verarbeitung

Es wird sichergestellt, dass die Daten im Falle einer Auftragsverarbeitung personenbezogener Daten nach den Anweisungen des Verantwortlichen verarbeitet werden.

Sicherheitsmaßnahmen bei der Übertragung von Daten

Es gelten Maßnahmen, die das unbefugte Lesen, Kopieren, Verändern oder Löschen von personenbezogenen

Daten während der Übertragung oder des Transports von Speichermedien verhindern.

- Alle Verbindungen zu unseren Rechenzentren werden während der Übertragung mit modernem TLS verschlüsselt. Die unterstützten Verschlüsselungen werden regelmäßig auf ihre Wertminderung überprüft.
- Dritte Parteien, die personenbezogene Daten verarbeiten, haben angemessene Sicherheitskontrollen eingerichtet.
- Unverschlüsselte E-Mail-Anhänge enthalten keine vertraulichen oder sensiblen Informationen.

Verfügbarkeit und Ausfallsicherheit

- Pläne zur Aufrechterhaltung des Geschäftsbetriebs und zur Wiederherstellung im Notfall sind vorhanden, werden getestet und regelmäßig aktualisiert.
- Zertifikate des Rechenzentrums: https://cloud.google.com/security/compliance/iso-27001/
- Cloudflare als Diensteanbieter für DDoS-Schutz

Sicherheitsmaßnahmen für den Fall von Zwischenfällen

- Es wurde ein dokumentiertes Verfahren für den Umgang mit Datenschutzvorfällen und -verletzungen eingeführt.
- Die Mitarbeiter werden regelmäßig darin geschult, wie sie Sicherheitsvorfälle verhindern können, aber auch, wie sie auf solche Vorfälle reagieren können, einschließlich der möglichen Notwendigkeit, Vorfälle den Behörden zu melden und die Benutzer zu informieren.
- Es wurde eine interne Hotline für Sicherheits- und Datenschutzvorfälle eingerichtet. Die Mitarbeiter werden ermutigt, Vorfälle zu melden.

Bewertungen der Sicherheitsmaßnahmen

Bewertungen und Tests der Wirksamkeit der wichtigsten organisatorischen, technischen und physischen Schutzmaßnahmen zum Schutz personenbezogener Daten werden gemäß unserer Richtlinien durchgeführt, die unter anderem Folgendes beinhalten:

- Externe Schwachstellen-Scans und Penetrationstests werden mindestens einmal im Jahr durchgeführt.
- Externe Infrastrukturprüfungen werden mindestens einmal im Jahr durchgeführt.
- Externe Code-Prüfungen werden durchgeführt, wenn dies notwendig erscheint.
- Interne Architektur- und Sicherheitsprüfungen werden mindestens einmal im Jahr durchgeführt.

Die Ergebnisse der Analysen werden dokumentiert.

Meister

Anhang 3 - Zugelassene Unterauftragsverarbeiter

Mit Abschluss dieses AVV stimmt der Verantwortliche einer Beauftragung der nachstehend angeführten Unterauftragsverarbeiter zu:

Unterauftragsverarbeiter		Beschreibung der Verarbeitung (*einschließlich einer klaren Unterscheidung der Zuständigkeiten, falls mehrere Unterauftragsverarbeiter zugelassen wurden*)	
Name	**Anschrift**		**Verarbeitungsregion**
Bereitstellung von Meister-Produkten			
Google Cloud EMEA Limited	70 Sir John Rogerson's Quay, Dublin 2, Ireland	Gewährleistung der **Produktbereitstellung** durch Produkt-Hosting in der Cloud-Region Europa.	Frankfurt a.M., Deutschland
MeisterLabs Software GmbH	Mariahilferstraße 97, 1060 Wien, Österreich	Gewährleistung der **Produktfunktionalität**, insbesondere durch Produktwartung und -entwicklung	Wien, Österreich
MongoDB Limited	Building 2, Number 1 Ballsbridge Shellbourne Road, Ballsbridge, D04 Y3X9, Dublin, Ireland	Gewährleistung der **Produktfunktionalität** durch Hosting bestimmter Anwendungsdatenbanken,	EU