Anlage 1 – Hauptvertrag (AGB)

Der Hauptvertrag besteht aus den AGB (*https://www.memomeister.com/agb/*) des Auftragsverarbeiters.

Anlage 2 – Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kreis der Betroffenen

Art der Verarbeitung: Erheben, Erfassen, Empfangen, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder die Verknüpfung, Einschränkung, Aktualisierung, Löschen oder die Vernichtung.

Die vorstehende Liste umschreibt die im Rahmen der Dienstleistung möglichen Verarbeitungstätigkeiten und die Art der personenbezogenen Daten:

Art der Daten	**Zweck der Daten Erhebung / Verarbeitung / Nutzung**	**Kreis der Betroffenen**
Bestandsdaten (Unternehmen) • Firmenname • Ansprechpartner • Telefonnummer • E-Mail • Straße, Hausnummer • Postleitzahl, Ort • Zahlungsdaten (nur wenn ein Bezahlabonnement besteht) • Vertragsdaten	• Kontakt/Ansprechpartner • Support • Zahlungsabwicklung • Rechnungsstellung	• Unternehmenskontakte • Interessenten • Abonnenten
Bestandsdaten (Nutzer) • Name • E-Mail • Telefonnummer (optional) • Handynummer (optional)	• Kontakt/Ansprechpartner • Zugriffs- und Zutrittskontrolle zur Software • Technischer Support	• Registrierte Nutzer • Mitarbeiter • Auszubildende, Praktikanten, Werkstudenten • Subunternehmer • Lieferanten • Registrierte Kunden
Während der Nutzung • Name • E-Mail • Telefonnummer (optional) • Handynummer (optional) • Standortdaten (optional) • Dokumente • Notizen & Texte • Bilder & Videos	• Login zur Software • Standorterkennung für Memos • Bereitstellung von gespeicherten Memos	• Registrierte Nutzer • Mitarbeiter • Auszubildende, Praktikanten, Werkstudenten • Subunternehmer • Lieferanten • Registrierte Kunden

Die vorstehende Liste umfasst Informationen von Kategorien betroffener Personen, deren Daten generell im Rahmen der Dienstleistung des Auftragsverarbeiters verarbeitet werden könnten. Angesichts der Art der Dienstleistung erkennt der Kunde an, dass der Auftragsverarbeiter die vorstehende Liste weder überprüfen noch pflegen kann. Der Kunde verpflichtet sich, den Auftragsverarbeiter über alle Änderungen an der vorstehenden Liste zu informieren per E-Mail an: datenschutz@memomeister.com

Anlage 3 – Technische und organisatorische Maßnahmen

Vom Auftragsverarbeiter umgesetzte und zugesicherte technische und organisatorische Maßnahmen:

Vertraulichkeit Art. 32 I b DSGVO

<table>
<tr>
<td>Zutrittskontrolle

Kein unbefugter Zutritt zu den Datenverarbeitungsanlagen</td>
<td>Sicherheitsvorkehrungen am Bürogebäude der Freiraum GmbH:

<table>
<tr><td>Schlüssel</td><td>X</td></tr>
<tr><td>Magnet- oder Chipkarten</td><td></td></tr>
<tr><td>Elektrische Türöffner</td><td></td></tr>
<tr><td>Alarmanlage</td><td></td></tr>
<tr><td>Videoanlage</td><td></td></tr>
<tr><td>Zaun</td><td></td></tr>
</table>
Personelle Sicherungen:
<table>
<tr><td>Werkschutz</td><td></td></tr>
<tr><td>Empfang</td><td>X</td></tr>
</table>
</td>
<td>Sicherheitsvorkehrungen am Server-Standort von AWS:

<table>
<tr><td>Schlüssel</td><td>X</td></tr>
<tr><td>Magnet- oder Chipkarten</td><td>X</td></tr>
<tr><td>Elektrische Türöffner</td><td>X</td></tr>
<tr><td>Alarmanlage</td><td>X</td></tr>
<tr><td>Videoanlage</td><td>X</td></tr>
<tr><td>Zaun</td><td>X</td></tr>
</table>
Personelle Sicherungen:
<table>
<tr><td>Werkschutz</td><td>X</td></tr>
<tr><td>Pförtner</td><td>X</td></tr>
</table>
</td>
</tr>
<tr>
<td>Zugangskontrolle

Kein unbefugter Zugang in Datenverarbeitungs-Systeme - EDV</td>
<td colspan="2">
<table>
<tr><td>Sichere Kennwörter</td><td>X</td></tr>
<tr><td>Automatische Sperrmechanismen</td><td>X</td></tr>
<tr><td>2-Faktor Authentifizierung</td><td>X</td></tr>
<tr><td>Verschlüsselung von Datenträgern</td><td>X</td></tr>
</table>
</td>
</tr>
<tr>
<td>Zugriffskontrolle

Innerhalb des Systems kein unbefugtes Lesen, kopieren, Verändern oder entfernen - EDV</td>
<td colspan="2">
<table>
<tr><td>Berechtigungskonzepte/ bedarfsgerechte Zugriffsrechte</td><td>X</td></tr>
<tr><td>Protokollierung von Zugriffen</td><td>X</td></tr>
</table>
</td>
</tr>
<tr>
<td>Trennungskontrolle

Getrennte Verarbeitung von Daten die zu unterschiedlichen Zwecken erhoben wurden - EDV</td>
<td colspan="2">
<table>
<tr><td>Mandantenfähigkeit (Gleichzeitiger Zugriff auf Software/ System ohne gegenseitigen Einblick)</td><td>X</td></tr>
<tr><td>Sandboxing (Bearbeitung in isolierten Bereichen)</td><td>X</td></tr>
</table>
</td>
</tr>
<tr>
<td>Pseudonymisierung

Daten können ohne Hinzuziehung zusätzlicher gesondert aufbewahrter und geschützter Information nicht einer bestimmten Person zugeordnet werden</td>
<td colspan="2">
<table>
<tr><td>Verarbeitung der Daten in pseudonymisierter Weise (Daten können nur durch „Schlüssel“ zugeordnet werden)</td><td>X</td></tr>
</table>
</td>
</tr>
</table>

Integrität Art. 32 I b DSGVO

Weitergabekontrolle Kein unbefugtes Lesen, kopieren, Verändern oder entfernen bei elektr. Übertragung und Transport - EDV	Verschlüsselung	X
	Virtual private networks (VPN)	X
	Elektronische Signatur	X
Eingabekontrolle Wann wurden welche Angaben wo eingegeben, verändert oder entfernt?	Protokollierung	X
	Dokumentenmanagement	X

Verfügbarkeit und Belastbarkeit Art. 32. I b, c DSGVO

Verfügbarkeitskontrolle Schutz gegen zufällige oder mutwillige Zerstörung oder Verlust	Backup – Strategie online/offline, onsite/ offsite	X
	Unterbrechungsfreie Stromversorgung	X
	Virenschutz	X
	Firewall	X
	Meldewege und Notfallpläne	X
	Rasche Wiederherstellbarkeit	X

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung Art. 32 I d, 25 I DSGVO

Datenschutz-Managementsystem	Datenschutzmanagementsystem	X
Incident-Response-Management (IRM)	Incident-Response Management	X
Datenschutzfreundliche Voreinstellungen	Datenschutzfreundliche Voreinstellungen	X
Auftragskontrolle Keine AV ohne Weisung des Auftragsgebers	Eindeutige Vertragsgestaltung	X
	Formalisiertes Auftragsmanagement	X
	Strenge Auswahl des Dienstleisters	X
	Vorabüberzeugungspflicht	X
	Nachkontrollen	X

Anlagen und Zertifikate:

Konkrete Beschreibung der TOMs (Freiraum GmbH und AWS)	X	SOC I/II/III (AWS)	X	ISO/IEC 27001:2013 (AWS)	X

Technische und organisatorische Maßnahmen (konkret)

Die Freiraum GmbH ist Anbieter einer digitalen Projektakte, die als Webservice erbracht wird. Die von der Freiraum GmbH in dem Zusammenhang getroffenen technischen und organisatorischen Maßnahmen sind nachfolgend beschrieben:

1. Allgemeine Informationen

Es gibt keine Server in den Büroräumen des Auftragsverarbeiter. Alle Server stehen in einem Rechenzentrum in Frankfurt am Main (Deutschland) das von Amazon Web Services betrieben wird. Weitere Informationen zu den Sicherheitsprozessen des AWS Rechenzentrums finden Sie hier:

- AWS Cloud Sicherheit
- AWS Datenschutz in Deutschland
- AWS Datenschutzhinweis
- AWS Übersicht über die Sicherheitsprozesse

2. Zutrittskontrolle

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

Die Büroräume der Freiraum GmbH befinden sich in einem Bürogebäude in Stuttgart. Der Eingang des Gebäudekomplexes ist über eine Zutrittstür gesichert, die stets beaufsichtigt oder verschlossen ist. Besucher werden immer durch mindesten einen Mitarbeiter der Freiraum GmbH begleitet.

Das Schlüsselmanagement für die Zutrittstür zum Gebäudekomplex liegt beim Vermieter. Die vom Vermieter ausgegebenen Schlüssel sind dem jeweiligen Mieter zugeordnet. Die Verwaltung der einzelnen Schlüssel der Freiraum GmbH für die Zutrittstür obliegt der Freiraum GmbH selbst. Diesbezüglich gibt es einen Prozess für die Ausgabe von Schlüsseln auf Basis eines 4-Augen-Prinzips. Die Ausgabe von Schlüsseln wird protokolliert. Mitarbeiter sind verpflichtet, einen Schlüsselverlust unverzüglich zu melden. Ferner gibt es einen Prozess bei einem Ausscheiden eines Mitarbeiters, der insbesondere auch die Rückgabe von Schlüsseln und sonstigem Eigentum der Freiraum GmbH durch den ausscheidenden Mitarbeiter beinhaltet.

Daten der Freiraum GmbH, die im Auftrag verarbeitet werden, werden ausschließlich im AWS-Rechenzentrum von Amazon in Frankfurt gespeichert. Dort sind folgende Maßnahmen zur Zutrittskontrolle getroffen: Das AWS-Rechenzentrum und die dort verwendeten Systeme sind in unscheinbaren Gebäuden untergebracht, die von außen nicht sofort als Rechenzentrum zu erkennen sind. Das Rechenzentrum selbst ist durch physische Sicherheitsmaßnahmen geschützt, um den unberechtigten Zutritt sowohl weiträumig (z. B. Zaun, Wände) als auch in den Gebäuden selbst zu verhindern. Der Zutritt zum Rechenzentrum wird durch elektronische Zugangskontrollen verwaltet und durch Alarmanlagen gesichert, die einen Alarm auslösen, sobald die Tür aufgebrochen oder aufgehalten wird. Die Zutrittsberechtigung wird von einer berechtigten Person genehmigt und innerhalb von 24 Stunden entzogen, nachdem ein Mitarbeiter- oder Lieferantendatensatz deaktiviert wurde. Alle Besucher müssen sich ausweisen und registrieren und werden stets von berechtigten Mitarbeitern begleitet. Zutritt zu sensiblen Bereichen wird durch Videoüberwachung überwacht. Ausgebildete Sicherheitskräfte bewachen das AWS-Rechenzentrum und die unmittelbare Umgebung davon 24 Stunden am Tag, 7 Tage die Woche.

3. Zugangskontrolle

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

Die Büroräume der Freiraum GmbH befinden sich im Erdgeschoss. Die Fenster sind dadurch potenziell von außen einsehbar. Die Bildschirme der Mitarbeiter sind jedoch stets so ausgerichtet, dass eine Einsichtnahme von außen nicht erfolgen kann.

An jedem IT-System, das bei der Freiraum GmbH im Einsatz ist, muss eine vorherige Authentifizierung erfolgen. Dies erfolgt auf Basis einer Zwei-Faktor-Authentifizierung (2FA). Dafür erfolgt der Anmeldeprozess (Authentifikation) mit Benutzerkennung und Passwort plus dynamisch erzeugtem Code der z.B. per SMS verschickt wird. Jede natürliche Person hat ein eigenes Benutzerkonto.

Eine Berechtigung zur Nutzung eines IT-Systems oder einer Applikation wird bei der Freiraum GmbH nach dem 4-Augen-Prinzip erteilt. Mitarbeiter erhalten nur Berechtigungen, die unbedingt erforderlich sind, damit dieser die ihm zugewiesenen Aufgaben erfüllen kann. Berechtigungen werden dabei auf das Minimale beschränkt. Erteilte Berechtigungen (und der Entzug) werden von der IT-Administration und systemseitig protokolliert. Der Vorgesetzte überprüft quartalsweise, ob die erteilten Berechtigungen noch erforderlich sind. Zudem überprüft er im Falle eines Aufgabenwechsels von Mitarbeitern, ob eine entsprechende Korrektur von Berechtigungen bei der IT-Administration zu beantragen ist. Im Falle des Ausscheidens eines Mitarbeiters entzieht die IT-Administration entsprechende Berechtigungen binnen 24 Stunden nach Ausscheiden eines Mitarbeiters.

Werden Initialpasswörter vergeben, ist bei der Freiraum GmbH stets vorgesehen, dass das Initialpasswort bei der ersten Anmeldung geändert wird. Dies wird technisch erzwungen. Bei der Freiraum GmbH gibt es Richtlinien zur Passwortverwendung, die ebenfalls grundsätzlich technisch erzwungen werden. Die Mindestpasswortlänge beträgt 12 Zeichen. Passwörter sind komplex zu wählen. Dies beinhaltet die Verwendung von Groß- und Kleinbuchstaben, Sonderzeichen und Ziffern, wobei mindestens 3 von 4 dieser Merkmale erfüllt sein müssen. Ein Passwortwechsel ist spätestens nach 365 Tagen zwingend. Es ist sichergestellt, dass die letzten 3 verwendeten Passwörter eines Nutzers nicht von diesem wiederverwendet werden können. Sollte sich der Stand der Technik bei der Verwendung von Passwörtern ändern, wird die Freiraum GmbH die Passwortrichtlinien entsprechend anpassen.

Ein Zugriff auf die externen IT-Systeme findet ausschließlich über verschlüsselte Verbindungen statt. Die dabei verwendeten Verschlüsselungsalgorithmen und Schlüssellängen entsprechen dem Stand der Technik. Für den Fall einer zertifikatsbasierten Zugriffstechnologie ist gewährleistet, dass die Zertifikate durch Mitarbeiter der IT-Administration verwaltet werden.

Alle IT-Systeme, mit denen Daten im Auftrag verarbeitet werden, sind mit Antivirus-Software ausgestattet. Jedes Arbeitsgerät hat einen passwortgesicherten Bildschirmschoner, der sich nach 5 Minuten Inaktivität automatisch aktiviert.

Für das AWS-Rechenzentrum gilt, dass auch dort alle Berechtigungen nach dem Prinzip der Minimalberechtigung erteilt und Berechtigungen regelmäßig überprüft werden. Die Vergabe und der Entzug von Berechtigungen werden protokolliert. Die Verwendung von Passwörtern ist ebenfalls geregelt und sieht die Verwendung von komplexen Passwörtern, einen Passwortwechsel nach spätestens 90 Tagen sowie eine Passworthistorie vor.

4. Zugriffskontrolle

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

Für die Erteilung von Benutzerrechten gilt bei der Freiraum GmbH ein Berechtigungskonzept. Dies sieht vor, dass Berechtigungen ausschließlich auf Basis des 4-Augenprinzips und nach dem Minimalprinzip vergeben werden. Dies beinhaltet, dass jeder Mitarbeiter nur die Berechtigungen erhält, die er unmittelbar benötigt, um seine Aufgaben im Unternehmen erfüllen zu können.

Das Berechtigungskonzept ist rollenbasiert. Jedem Mitarbeiter wird grundsätzlich eine bestimmte Rolle zugewiesen. Von dieser Rolle abweichende Berechtigungen müssen begründet sein. Der Zugriff auf personenbezogenen Daten (Lesen, Ändern, Löschen), wird protokolliert, dabei wird die IP-Adresse sowie der Zeitpunkt der getätigten Systemaktivität gespeichert. Jedem Login ist eine Person zugeordnet.

Die Vergabe und der Entzug von Berechtigungen wird protokolliert. Eine quartalsweise Überprüfung erfolgt durch die IT-Administration in Zusammenarbeit mit den Vorgesetzten der Mitarbeiter. Der Zugriff auf den AWS-Server erfolgt über eine private Schlüsseldatei (Private Key File). Die zuständigen Mitarbeiter des Auftragsverarbeiter erhalten jeweils einen eigenen Key.

5. 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.

Dadurch, dass Berechtigungen nach dem Minimalprinzip vergeben werden, ist gewährleistet, dass der Kreis der Personen, die Zugang zu Daten haben, die im Auftrag verarbeitet werden, beschränkt ist. Ein Kopieren von Daten auf externe Datenträger ist systemseitig unterbunden. Ein Export von Daten wird auf Applikationsebene protokolliert und für einen Zeitraum von 12 Monaten unter Angabe der jeweiligen Benutzerkennung gespeichert.

Jeder Zugriff auf und der Abruf von Daten der Applikation erfolgt verschlüsselt (TLS).

Sofern Daten im Einzelfall auf Anfrage des Auftraggebers an diesen durch die Freiraum GmbH übergeben werden soll, werden die Parteien im Voraus eine Verschlüsselungsmethode bzw. einen Weg der sicheren Übertragung vereinbaren. Zur Sicherstellung der Integrität kommen elektronische Signaturen zum Einsatz. Die Übertragung von Passwort und Nutzerdaten an AWS erfolgt ausschließlich über verschlüsselte SSL-Verbindungen.

6. Eingabekontrolle

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

Jede Eingabe von Daten, die im Auftrag des Auftraggebers von der Freiraum GmbH verarbeitet werden, wird systemseitig unter Zuordnung der jeweiligen Benutzerkennung protokolliert. Gleiches gilt für die Änderung und Löschung von Daten. Im Falle einer Änderung von Daten ist aus der Protokollierung erkenntlich, welche Änderungen vorgenommen wurden. Die Protokolle werden für die Dauer der Vertragslaufzeit von der Freiraum GmbH gespeichert. Eine vorherige Löschung kann zwischen den Parteien vereinbart werden. Durch die Protokollierung ist jederzeit nachvollziehbar, welche Benutzer Daten eingegeben, geändert oder gelöscht hat.

Änderungen/Eingaben von personenbezogenen Daten direkt in der Auftragsverarbeiter-Datenbank bei AWS werden aufgezeichnet, genauso wie externe Zugriffe von Nutzern (Logfile für Logins). AWS zeichnet Netzwerkzugriffe auf, inklusive Zeitstempel und IP-Adresse. Auch Zugriffsversuche werden aufgezeichnet, inklusive Zeitstempel, Nutzername und Zieldatenbank.

7. Auftragskontrolle

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

Der Schutz personenbezogener Daten und auch der Schutz von Betriebs- und Geschäftsgeheimnissen hat bei der Freiraum GmbH eine hohe Priorität. Alle Mitarbeiter sind auf Vertraulichkeit verpflichtet. Es gibt einen externen Datenschutzbeauftragten, der auch die regelmäßige Schulung der Mitarbeiter plant und durchführt. Alle Mitarbeiter erhalten mindestens alle zwei Jahre eine Datenschutzschulung bzw. eine entsprechende „Auffrischung“.

Mitarbeiter, die an der Erbringung von Leistungen für den Auftraggeber beteiligt sind, sind im Hinblick auf die Verarbeitung der Daten instruiert. Sofern der Auftraggeber ergänzende Weisungen erteilt, wird die Freiraum GmbH alle betroffenen Mitarbeiter unverzüglich über die jeweilige Weisung informieren und Handlungsanweisungen zur Umsetzung geben.

Die Datenschutzvorkehrungen der Freiraum GmbH beinhalten auch eine regelmäßige Überprüfung und Bewertung der Verträge mit Unterauftragnehmern und der getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit. Hierzu gehört auch ein Verbesserungs- und Vorschlagswesen, an dem sich Mitarbeiter beteiligen können. Die Freiraum GmbH gewährleistet so eine kontinuierliche Verbesserung der Prozesse im Umgang mit personenbezogenen Daten.

Mit AWS wurden die allgemeinen Geschäftsbedingungen und gesetzliche Regelungen zur Auftragsverarbeitung vereinbart. Die Daten werden physisch in Deutschland gespeichert und nicht in Drittländer übermittelt. AWS hat sich dem Auftragsverarbeiter gegenüber innerhalb einer Datenverarbeitungs-Vereinbarung zur Wahrung von Datenschutzstandards nach EU-Recht verpflichtet. Diese Verpflichtung unterliegt allerdings der Geheimhaltung. Die Rechte an den vorgehaltenen Daten liegen beim Auftragsverarbeiter und nicht bei AWS.

8. Verfügbarkeitskontrolle

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

Alle Daten, die für den Auftraggeber verarbeitet werden, befinden sich im AWS-Rechenzentrum in Frankfurt. Die Freiraum GmbH hat Maßnahmen getroffen, die eine Sicherung der Daten und Wiederherstellung von Daten gewährleistet. Die Datenhaltung erfolgt zudem redundant. Es gibt ein Datensicherungs- und Wiederherstellungskonzept, dessen Wirksamkeit regelmäßig getestet wird.

Im AWS-Rechenzentrum sind umfangreiche Maßnahmen zur Gewährleistung der Verfügbarkeit getroffen. Im Rechenzentrum ist eine automatische Branderkennung und -bekämpfung installiert. Das Branderkennungssystem setzt Rauchsensoren in der gesamten Umgebung der Rechenzentren, in mechanischen und elektrischen Bereichen der Infrastruktur, Kühlräumen und sowie in den Räumen, in denen die Generatoren untergebracht sind, ein. Alle Stromversorgungssysteme dort sind redundant. Eine unterbrechungsfreie Stromversorgung (USV) sorgt im Fall eines Stromausfalls dafür, dass kritische Bereiche der Anlage weiterhin mit Strom versorgt werden. Das Rechenzentrum verfügt darüber hinaus über Generatoren, die die gesamte Anlage mit Notstrom versorgen können. Das Rechenzentrum verfügt über eine Klimatisierung und Temperaturkontrolle. Es werden vorbeugende Wartungsmaßnahmen durchgeführt, um den fortlaufenden Betrieb der Anlagen zu gewährleisten.

9. Trennungsgebot

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

Die IT-Systeme, auf denen Daten im Auftrag verarbeitet werden, sind mandantenfähig. Es ist sichergestellt, dass Daten getrennt voneinander verarbeitet werden. Hierbei ist die Trennung von Systemdateien unterschiedlicher Anwendungen und die Trennung von Benutzerdateien verschiedener Benutzer gewährleistet.

Anlage 4 – Liste der Unterauftragsverarbeiter

Eine Liste der vom Auftragsverarbeiter, mit Zustimmung des Auftraggebers, eingesetzten Unterauftragsverarbeiter.

Unterauftragnehmer	Anschrift / Land	Leistung
Amazon Web Services Inc. (“AWS Frankfurt”)	410 Terry Avenue North, Seattle WA 98109, United States Speicherstandort: Deutschland	Hosting und Betriebsaufgaben
Zoho Corporation B.V.	Hoogoorddreef 15, 1101BA, Amsterdam, Niederlande	Kundenbeziehungsmanagement, Kundensupport
MailerLite Limited	71 Lower Baggot Street, Dublin 2, D02 P593, Irland	Automatisierte Kommunikation mit Kunden
Google Ireland Limited	Gordon House, Barrow Street, Dublin 4, Irland	Interne und externe Kommunikation über E-Mail und Google Workspace, Error Monitoring
MongoDB Inc.	Building Two, Number One Ballsbridge, Dublin 4, Irland	MongoDB Datenbank Verwaltung basierend auf Amazon Web Services Infrastruktur