# Data Processing Agreement

## 1. Gegenstand der Datenverarbeitung

1.1. Im Rahmen des zwischen den Parteien geschlossenen Vertrages ist es nicht ausgeschlossen, dass der Auftragnehmer personenbezogene Daten des Auftraggebers oder dessen Vertragspartner im Auftrag des Auftraggebers verarbeitet, über deren Verarbeitung der Auftraggeber als Verantwortlicher entscheidet (nachfolgend Daten). Diese Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag (nachfolgend Vereinbarung) konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien.

## 2. Gegenstand, Art, Zweck und Laufzeit der Auftragsverarbeitung

2.1. Der Auftragnehmer verarbeitet die Daten gem. Art. 28 Verordnung (EU) 2016/679 (Datenschutzgrundverordnung, nachfolgend DSGVO) im Auftrag und nach Weisung des Auftraggebers.

2.2. Die Verarbeitung der Daten im Rahmen der Auftragsverarbeitung erfolgt entsprechend den in Anlage 1 enthaltenen Festlegungen zu Art, Umfang und Zweck der Datenverarbeitung. Sie bezieht sich auf die in Anlage 1 festgelegten Arten von Daten und den dort genannten Kategorien von betroffenen Personen. Ergänzend dazu ergeben sich Art und Umfang der Verarbeitung auch aus dem Hauptvertrag.

2.3.Die Verarbeitung der Daten findet im Gebiet der Bundesrepublik Deutschland, in einem anderen Mitgliedstaat der Europäischen Union (EU) oder in einem Staat des Europäischen Wirtschaftsraums (EWR) statt. Der Auftragnehmer darf Daten unter Einhaltung dieser Vereinbarung und der Art. 44 ff. DSGVO auch außerhalb des EWR verarbeiten.

2.4. Die Dauer dieser Vereinbarung (nachfolgend: Laufzeit) richtet sich nach dem Hauptvertrag.

## 3. Weisungsbefugnisse des Auftraggebers

3.1. Der Auftragnehmer verarbeitet die Daten ausschließlich in Übereinstimmung mit den Weisungen des Auftraggebers, wie sie in dieser Vereinbarung und dem Hauptvertrages festgelegt sind. Einzelweisungen, die von den Festlegungen dieser Vereinbarung oder des Hauptvertrags wesentlich abweichen oder zusätzliche Anforderungen aufstellen, bedürfen der vorherigen Zustimmung des Auftragnehmers. Einzelweisungen sind vom Auftragnehmer in Textform zu dokumentieren.

3.2. Ist der Auftragnehmer der Ansicht, dass eine Einzelweisung gegen geltendes Datenschutzrecht verstößt, wird er den Auftraggeber unverzüglich darauf hinweisen; der Auftragnehmer ist im Falle einer offensichtlich rechtswidrigen Einzelweisung nicht an diese Einzelweisung gebunden, im Übrigen ist er

berechtigt, die Ausführung der Weisung bis zur Bestätigung der Weisung durch den Auftraggeber auszusetzen.

# 4. Pflichten des Auftraggebers

4.1. Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung sowie für die Wahrung der Rechte der Betroffenen verantwortlich. Der Auftraggeber hat die alleinige Weisungsbefugnis gegenüber dem Auftragnehmer in Bezug auf die Verarbeitung der Daten.

4.2. Der Auftraggeber hat den Auftragnehmer unverzüglich zu informieren, wenn er in Bezug auf die Leistungen des Auftragnehmers Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen oder seinen Weisungen feststellt.

# 5. Pflichten des Auftragnehmers

5.1. Der Auftragnehmer stellt sicher und kontrolliert regelmäßig, dass die Verarbeitung gemäß Hauptvertrag in seinem Verantwortungsbereich, den der Unterauftragnehmer einschließt, in Übereinstimmung mit den Bestimmungen dieser Vereinbarung erfolgt.

5.2. Der Auftragnehmer darf ohne vorherige Zustimmung durch den Auftraggeber im Rahmen der Auftragsverarbeitung keine Daten zu eigenen Zwecken verarbeiten. Dies gilt nicht, und ein Weisungsrecht des Auftraggebers besteht insofern nicht, sofern der Auftragnehmer durch geltendes Recht zu einer Datenverarbeitung verpflichtet ist; in solch einem Fall teilt der Auftragnehmer dem Auftraggeber dies vor der Verarbeitung mit, sofern das geltende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

5.3. Der Auftragnehmer unterstützt den Auftraggeber bei behördlichen Aufsichtsverfahren bezüglich der Verarbeitung durch den Auftragnehmer, sofern dies erforderlich und dem Auftragnehmer zumutbar ist.

5.4. Der Auftragnehmer hat die bei der Verarbeitung beschäftigten Personen zur Vertraulichkeit zu verpflichten, sofern dies nicht bereits geschehen ist oder sofern diese Personen nicht vergleichbaren angemessenen gesetzlichen Verschwiegenheitsverpflichtungen unterliegen.

5.5. Der Auftragnehmer ist verpflichtet, einen Datenschutzbeauftragten zu bestellen, sofern und solange die gesetzlichen Voraussetzungen für eine Bestellpflicht gegeben sind.

5.6. Der Auftragnehmer unterstützt den Auftraggeber, damit der Auftraggeber seinen Pflichten aus Art. 32 DSGVO und auf Anfrage ggf. aus Art. 35 DSGVO (Datenschutz-Folgenabschätzung) sowie Art. 36 DSGVO (Konsultation der Aufsichtsbehörde) nachkommen kann, sofern dies dem Auftragnehmer zumutbar ist.

5.7. Der Auftragnehmer stellt dem Auftraggeber auf dessen Anfrage in Textform alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung.

# 6. Technische und organisatorische Maßnahmen

6.1. Der Auftragnehmer hat spätestens zu Beginn der Datenverarbeitung die in Anlage 2 aufgelisteten technischen und organisatorischen Maßnahmen umzusetzen und während der Laufzeit aufrechtzuerhalten. Bei diesen Maßnahmen handelt es sich um solche der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit und der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen gem. Art. 32 Abs. 1 DSGVO zu berücksichtigen.

6.2. Dem Auftragnehmer ist es gestattet, alternative technische und organisatorische Maßnahmen umzusetzen, sofern dabei das Sicherheitsniveau der Maßnahmen in Anlage 2 nicht unterschritten wird. Wesentliche Änderungen bedürfen der vorherigen Zustimmung des Auftraggebers in Textform.

# 7. Mitzuteilende Verstöße des Auftragnehmers

7.1. Der Auftragnehmer informiert den Auftraggeber im Falle einer Verletzung des Schutzes von Daten unverzüglich, wenn er feststellt, dass er oder einer seiner Mitarbeiter bei der Verarbeitung gegen datenschutzrechtliche Vorschriften oder diese Vereinbarung verstoßen hat.

7.2. Der Auftragnehmer unterstützt den Auftraggeber, damit der Auftraggeber seinen Meldepflichten wegen Datenpannen nach Art. 33 f. DSGVO nachkommen kann, sofern dies dem Auftragnehmer zumutbar ist. Der Auftraggeber erstattet dem Auftragnehmer etwaige hierdurch entstehenden, nachzuweisenden Aufwände und Kosten.

# 8.Kontrollrechte des Auftraggebers

8.1. Der Auftraggeber ist berechtigt, nach rechtzeitiger Ankündigung, im Rahmen der üblichen Geschäftszeiten auf eigene Kosten, ohne Störung des Betriebsablaufs und unter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen und sonstigen Geheimhaltungsverpflichtungen des Auftragnehmers die Geschäftsräume des Auftragnehmers, in denen Daten verarbeitet werden, zu betreten, um sich von der Einhaltung der Maßnahmen gem. § 6 zu überzeugen. Der Auftraggeber ist berechtigt, diese Prüfung durch einen zur Vertraulichkeit verpflichteten Dritten durchführen zu lassen. Diese Berechtigung ist beschränkt auf die Räumlichkeiten des Auftragnehmers und erstreckt sich nicht auf die Räumlichkeiten von Dritten (z.B. von Hetzner oder anderen Clouddiensteanbietern), selbst wenn dort Daten des Auftraggebers verarbeitet werden.

8.2. Der Auftragnehmer gewährt dem Auftraggeber oder einem von diesem beauftragten Dritten die zur Durchführung der Kontrollen erforderlichen Zugangs-, Auskunfts- und Einsichtsrechte und wirkt bei der Kontrolle in angemessenem Umfang mit.

8.3. Der Auftragnehmer ist berechtigt, Informationen nicht zu offenbaren, die sensibel im Hinblick auf die Geschäfte des Auftragnehmers sind oder wenn der Auftragnehmer durch deren Offenbarung gegen gesetzliche oder andere vertragliche Verpflichtungen verstoßen würde.

8.4. Der Auftraggeber hat den Auftragnehmer unverzüglich über alle mit der Durchführung der Kontrolle zusammenhängenden Umstände zu informieren. Der Auftraggeber darf in der Regel eine Kontrolle pro Jahr durchführen. Dem Auftraggeber bleiben weitere Kontrollen im Fall besonderer Vorkommnisse nachgelassen.

8.5. Der Auftragnehmer erhält vom Auftraggeber eine pauschale Aufwandsentschädigung für seinen im Rahmen dieser Kontrollen anfallenden Aufwand in Höhe von EUR 1,800 pro Tag der Kontrolle. Dies gilt nicht, wenn der Auftragnehmer den Anlass der Kontrolle schuldhaft zu verantworten hat. Dem Auftraggeber bleibt nachgelassen, dass der Aufwand nicht oder in geringerer Höhe angefallen ist.

8.6. Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Kontrolle, hat der Auftraggeber den Dritten schriftlich ebenso zu verpflichten, wie auch der Auftraggeber aufgrund von § 8 gegenüber dem Auftragnehmer verpflichtet ist. Der Auftraggeber hat den Dritten nachweislich auf Vertraulichkeit zu verpflichten, es sei denn, dass der Dritte einer gesetzlichen Verschwiegenheitsverpflichtung unterliegt.

8.7. Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der Maßnahmen nach § 6 auch durch die Vorlage eines geeigneten Testats, von Berichten unabhängiger Instanzen oder einer Zertifizierung durch Datenschutzaudit erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber ermöglicht, sich von der Einhaltung dieser Maßnahmen zu überzeugen. § 8 (1) bleibt unberührt.

# 9. Unterauftragnehmer

9.1. Der Auftragnehmer darf geeignete Unterauftragnehmer mit der Verarbeitung von Daten betrauen, wenn der Auftraggeber dem im Einzelfall in Textform einwilligt. Der Auftragnehmer willigt darüber hinaus in den Einsatz der in Anlage 3 genannten Unterauftragnehmer ein.

9.2. Unterauftragsverhältnisse im Sinne dieser Vereinbarung sind nur solche Dienstleistungen, die sich auf den Hauptvertrag beziehen und eine Datenverarbeitung zum Gegenstand haben. Keiner Zustimmung bedarf die Beauftragung von Unterauftragnehmern, bei denen der Unterauftragnehmer lediglich eine Nebenleistung zur Unterstützung bei der Erfüllung des Hauptvertrags in Anspruch nimmt (z.B. Post-, Transport-, Telekommunikationsdienste wie Asana oder Slack).

9.3. Der Auftragnehmer wird den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder den Austausch von Unterauftragnehmer informieren. Der Auftraggeber kann der Hinzuziehung oder dem Austausch von Unterauftragnehmer in Textform innerhalb einer Frist von 14 Tagen nach Information durch den Auftragnehmer aus wichtigem Grund widersprechen.

9.4. Dem Unterauftragnehmer werden die im Wesentlichen gleichen Datenschutzpflichten auferlegt, die in dieser Vereinbarung festgelegt sind. Insbesondere ist sicherzustellen, dass die technischen und organisatorischen Maßnahmen vom Unterauftragnehmer so durchgeführt werden, dass die Verarbeitung

entsprechend den Anforderungen des Datenschutzrechts erfolgt. Der Auftragnehmer haftet für seine Unterauftragnehmer gegenüber dem Auftraggeber gem. § 278 BGB.

9.5. Der Auftragnehmer darf auch Unterauftragnehmer in Drittstaaten einsetze. In diesem Fall gelten § 9 Abs. 1 bis 3 dieser Vereinbarung entsprechend und es müssen die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sein. Der Auftraggeber bevollmächtigt den Auftragnehmer hiermit, in Vertretung des Auftraggebers mit einem Unterauftragnehmer , der Daten außerhalb der EU bzw. des EWR verarbeitet, einen Vertrag unter Einbeziehung von Standarddatenschutzklauseln für die Übermittlung von Daten an Auftragsverarbeiter in Drittländern zu schließen, sofern kein Angemessenheitsbeschluss der EU-Kommission vorliegt.

9.6. Die Regelungen der vorstehenden Absätze gelten auch, wenn der Unterauftragnehmer seinerseits einen Unterauftragnehmer einschaltet.

# 10. Rechte der Betroffenen

10.1. Die Rechte der durch die Verarbeitung betroffenen Personen sind gegenüber dem Auftraggeber geltend zu machen. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Geltendmachung seiner Rechte wenden sollte, wird der Auftragnehmer dieses Ersuchen an den Auftraggeber weiterleiten.

10.2. Für den Fall, dass ein Betroffener gegenüber dem Auftraggeber berechtigte datenschutzrechtliche Ansprüche geltend macht, wird der Auftragnehmer den Auftraggeber bei der Erfüllung dieser Ansprüche mit geeigneten technischen und organisatorischen Maßnahmen im Rahmen des rechtlich und tatsächlich Möglichen unterstützen, sofern dies für den Auftragnehmer nicht unzumutbar ist. § 8 Abs. (5) gilt entsprechend.

# 11. Rückgabe und Löschung überlassener Daten und Datenträger

11.1. Der Auftragnehmer hat Daten nach Ende der Laufzeit nach Wahl des Auftraggebers zu löschen und/oder, sofern sie auf physischen Datenträgern übermittelt worden waren, zurückzugeben, es sei denn, der Auftragnehmer ist zu einer Speicherung verpflichtet. Der Auftragnehmer hat an den Daten kein Zurückbehaltungsrecht, es sei denn, sein Gegenanspruch ist rechtskräftig festgestellt oder unbestritten.

11.2. Dokumentationen, die dem Nachweis der ordnungsgemäßen Verarbeitung oder gesetzlichen Aufbewahrungsfristen dienen, dürfen vom Auftragnehmer im Rahmen der Gesetze über Ende der Laufzeit hinaus aufbewahrt werden

# 12. Verhältnis zum Hauptvertrag, Rechtswahl

12.1. Soweit in dieser Vereinbarung keine Sonderregelungen enthalten sind, gelten die Bestimmungen des Hauptvertrags. Im Fall von Widersprüchen zwischen diesem Vertrag und sonstigen Vereinbarungen der Parteien gehen die Regelungen aus dieser Vereinbarung vor.

12.2. Es gelten die DSGVO und ergänzend deutsches Recht.

# Anhang 1

## Details zu den Auftraggeber-Daten und der Verarbeitung

| **Thema** | **Beschreibung** |
|---|---|
| Vertragsgegenstand | Zurverfügungstellung einer webbasierten Software & Datenbankzugriff samt Wartung und Support, sowie Ad Hoc Data Intelligence Dienstleistungen |
| Dauer | Für die Dauer des Hauptvertrages |
| Natur und Zweck | Die personenbezogenen Daten werden Zwecks Erfüllung der Aufträge des und Kommunikation mit dem Verantwortlichen verarbeitet. |
| Art der personenbezogenen Daten | E-Mail-Adressen, IP-Adressen, Name |
| Kategorien betroffener Personen | Mitarbeiter & Kunden des Verantwortlichen |

# Anhang 2

## Technische und organisatorische Maßnahmen (Art 32 Abs 1 DSGVO)

### 1. Pseudonymisierung und Verschlüsselung personenbezogener Daten

- Pseudonymisierung personenbezogener Daten
- Verschlüsselung personenbezogener Daten

Erklärung:

Maßnahmen der Pseudonymisierung:

- Vermeidung der Speicherung von IP-Adressen, notfalls Kürzung von IP-Adressen
- Vermeidung der Speicherung von Cookie-IDs

Verschlüsselung personenbezogener Daten:

- Zugang zur Anwendung ist nur über verschlüsselte Übertragungswege und durch Login mittels Username und Passwort möglich

## 2. Zugangskontrolle

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

☒ Zuordnung von Benutzerrechten
☒Erstellen von Benutzerprofilen
☒ Passwortvergabe
☐ Authentifikation mit biometrischen Verfahren
☒ Authentifikation mit Benutzername / Passwort
☒ Zuordnung von Benutzerprofilen zu IT-Systemen
☐ Einsatz einer Hardware-Firewall
☒ Einsatz von VPN-Technologie
☐ Sperren von externen Schnittstellen (USB etc.)
☒ Einsatz einer Software-Firewall
☒ Verschlüsselung von Datenträgern in Laptops / Notebooks
☒ Verzicht auf Einsatz von mobilen Datenträgern zur Speicherung personenbezogener Daten
☒ Verschlüsselung von Smartphone-Inhalten
☒ Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)
☒ Einsatz von Anti-Viren-Software

## 3. 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.
☒ Erstellen eines Berechtigungskonzepts
☒ Verwaltung der Rechte durch Systemadministrator
☒ Anzahl der Administratoren auf das „Notwendigste“ reduziert
☒ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
☒ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
☐ Sichere Aufbewahrung von Datenträgern
☐ Physische Löschung von Datenträgern vor Wiederverwendung
☐ Ordnungsgemäße Vernichtung von Datenträgern
☒ Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
☐ Protokollierung der Vernichtung
☒ Verschlüsselung von Datenträgern

## 4. 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.

☒ Protokollierung der Eingabe, Änderung und Löschung von Daten
☐ Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

## 5. Auftragskontrolle

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

☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
☐ vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
☒ schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsverarbeitungsvertrag)
☒ Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
☒ Auftragnehmer hat Datenschutzbeauftragten bestellt
☐ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
☐ Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
☐ laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
☐ Vertragsstrafen bei Verstößen

## 6. Verfügbarkeitskontrolle

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

☒ Daten werden nur in Datenzentren von Anbietern gespeichert, die eine ISO 27001 oder gleichwertige Zertifizierung vorweisen können

Zu den Maßnahmen, die dort getroffen werden, gehören üblicherweise:

☒ Unterbrechungsfreie Stromversorgung (USV)

☒ Klimaanlage in Serverräumen
☒ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
☒ Schutzsteckdosenleisten in Serverräumen
☒ Feuer- und Rauchmeldeanlagen
☒ Feuerlöschgeräte in Serverräumen
☒ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
☒ Erstellen eines Backup- & Recovery-Konzepts
☒ Testen von Datenwiederherstellung
☒ Erstellen eines Notfallplans
☒ Redundante Aufbewahrung von Datensicherung in der Cloud
☒ Serverräume nicht unter sanitären Anlagen
☒ In Hochwassergebieten: Serverräume über der Wassergrenze

### 7. Trennungsgebot

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

☐ physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
☒ Logische Mandantentrennung (softwareseitig)
☒ Erstellung eines Berechtigungskonzepts
☐ Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
☐ Versehen der Datensätze mit Zweckattributen/Datenfeldern
☐ Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System
☒ Festlegung von Datenbankrechten
☒ Trennung von Produktiv- und Testsystem

# Anhang 3

## Genehmigte Unterauftragsverarbeiter/Unterauftragnehmer

- Freshdesk GmbH
- Google Ireland Limited
- Hetzner Online GmbH
- Amazon Web Services EMEA SARL, NL Deutschland
- HubSpot Germany GmbH
- Userflow Inc.