# Auftragsverarbeitungsvertrag

**Auftragnehmer/Auftragsverarbeiter**

| | |
|---|---|
| Firmenname: | Heyflow GmbH |
| Straße, Nr: | Jungfernstieg 49 |
| PLZ, Stadt: | 20354 Hamburg |

**Auftraggeber/Verantwortlicher**

| | |
|---|---|
| Firmenname: | _____ |
| Straße, Nr.: | _____ |
| PLZ, Stadt: | _____ |

## Präambel

Die Parteien haben einen Vertrag abgeschlossen, nach dem der Auftragnehmer Services für den Auftraggeber erbringt.

Bei der Leistungserbringung verarbeitet der Auftragnehmer als Auftragsverarbeiter (Artikel 4 Nr. 8 DS-GVO) im Auftrag des Auftraggebers als Verantwortlichen (Artikel 4 Nr. 7 DS-GVO) personenbezogene Daten (Artikel 4 Nr. 1 DS-GVO).

## 1. Begriffsbestimmungen

**1.1** **Für die Zwecke dieses Auftragsverarbeitungsvertrags finden die Begriffsbestimmungen des Artikel 4 DS-GVO Anwendung, sofern nachfolgend nicht etwas anderes bestimmt ist.**

**1.2** **Für die Zwecke dieses Auftragsverarbeitungsvertrags, finden die folgenden abweichenden und/oder zusätzlichen Begriffsbestimmungen Anwendung:**

1.2.1 „Drittland" ist jedes Land außerhalb des EWR.

1.2.2 „Endnutzer" meint denjenigen Nutzer, der den vom Auftraggeber eingesetzten Flow nutzt.

1.2.3 „EU" oder „Union" ist die Europäische Union.

1.2.4 „EWR" ist der Europäische Wirtschaftsraum.

1.2.5 Ein „Flow" ist ein web-basiertes, interaktives Anfrageformular, das über den vom Auftragnehmer angebotenen Software-Baukasten durch den Auftraggeber eigenverantwortlich konfiguriert werden kann.

1.2.6 „Hauptvertrag" sind die allgemeinen Geschäftsbedingungen.

1.2.7 „Mitgliedstaat" ist ein Mitgliedstaat der EU und/oder Vertragsstaat des EWR.

1.2.8 „Parteien" (oder einzeln eine „Partei") sind der Auftraggeber und Auftragnehmer.

1.2.9 „Services" und Dienste sind die vom Auftragnehmer für den Auftraggeber im Rahmen des Hauptvertrages zu erbringenden Leistungen, wie in den allgemeinen Geschäftsbedingungen beschrieben.

1.2.10 „Sichere Drittländer" sind alle Drittländer, für die ein Angemessenheitsbeschluss der Europäischen Kommission gemäß Artikel 45 (3) DS-GVO gilt.

1.2.11 „Standardvertragsklauseln (Auftragsverarbeiter)" sind die Standardvertragsklauseln, die dem Beschluss der Europäischen Kommission 2021/914 vom 4. Juni 2021 (Az. C(2021) 3972, ABl. EU Nr. L 199/31 vom 07.06.2021) über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates, anhängen (Modul 2).

1.2.12 „Unterauftragsverarbeiter" ist jeder weitere Auftragsverarbeiter, den ein Auftragsverarbeiter gemäß Artikel 28 (2) und (4) DS-GVO in Anspruch nimmt.

1.2.13 „Verbundenes Unternehmen" ist ein Unternehmen, (a) in dessen Eigentum oder unter dessen Kontrolle der Auftraggeber oder der Auftragnehmer steht, (b) das im Eigentum oder unter der Kontrolle des Auftraggebers oder des Auftragnehmers steht oder (c) das unter gemeinsamer Kontrolle oder gemeinsamem Eigentum mit dem Auftraggeber oder Auftragnehmer steht. Kontrolle bedeutet die Möglichkeit, entweder durch Stimmrechte, vertraglich oder auf andere Weise unmittelbar oder mittelbar beherrschenden Einfluss auf ein Unternehmen auszuüben.

# 2. Anwendungsbereich, Parteien und ihre jeweiligen Rollen

2.1 Dieser Auftragsverarbeitungsvertrag findet Anwendung auf die Verarbeitung personenbezogener Daten durch den Auftragnehmer bei der Erbringung der Services.

2.2 Der Auftragnehmer stellt dem Auftraggeber einen Software-Baukasten zur Erstellung von Flows zur Verfügung. Grundsätzlich obliegt die Ausgestaltung der Flows durch die Verwendung des Baukastens dem Auftraggeber. Der Auftragnehmer kann die Art, der durch einen Flow erhobenen Daten nicht pauschal eingrenzen. Der Auftragnehmer stellt dem Auftraggeber eine optional zu verwendende Produktfunktionalität zur Verfügung, die die Speicherung von personenbezogenen Daten von Endnutzern durch

den Auftragnehmer verhindert. Die sachgemäße Verwendung der entsprechenden Funktion obliegt dem Auftraggeber.

# 3. Details der Verarbeitung

Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten und Kategorien betroffener Personen, sowie Ort der Verarbeitung sind in Anhang 1 dieses Auftragsverarbeitungsvertrags festgelegt.

# 4. Pflichten und Rechte des Verantwortlichen

## 4.1 Verantwortlichkeiten des Verantwortlichen

Der Verantwortliche ist für die Einhaltung der nach der DS-GVO auf einen Verantwortlichen anwendbaren Verpflichtungen verantwortlich, insbesondere für die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten gemäß Kapitel II DS-GVO und die Einhaltung der Rechte der Betroffenen gemäß Kapitel III DS-GVO.

## 4.2 Recht Weisungen zu erteilen

4.2.1 Der Verantwortliche behält sich das Recht vor, Weisungen an den Auftragsverarbeiter bezüglich der Verarbeitung personenbezogener Daten unter diesem Auftragsverarbeitungsvertrag zu erteilen.

4.2.2 Die Regelungen dieses Auftragsverarbeitungsvertrags, insbesondere die Bestimmung der Details der Verarbeitung gemäß Abschnitt 3, dienen als allgemeine Weisungen, personenbezogene Daten so zu verarbeiten, wie es für die Erbringung der Services vernünftigerweise erforderlich ist und mit diesem Auftragsverarbeitungsvertrag und dem Hauptvertrag vereinbart ist.

4.2.3 Der Verantwortliche ist befugt, Einzelweisungen in Textform oder durch entsprechende Einstellungen im Software-Baukasten zu erteilen.

## 4.3 Recht auf Auskunft und auf Durchführung von Überprüfungen, einschließlich Inspektionen

4.3.1 Der Verantwortliche hat das Recht, vom Auftragsverarbeiter alle erforderlichen Informationen zum Nachweis der Einhaltung der in Artikel 28 DS-GVO niedergelegten Pflichten zu verlangen und Überprüfungen – einschließlich Inspektionen – beim Auftragsverarbeiter entweder selbst oder durch einen von ihm beauftragten Prüfer durchzuführen.

4.3.2 Zum Nachweis der Einhaltung seiner Pflichten kann der Auftragsverarbeiter aktuelle Bescheinigungen, Berichte oder Auszüge aus Berichten von unabhängigen Stellen (z.B. Wirtschaftsprüfer, interne Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung,

Datenschutzprüfer, Qualitätsprüfer) oder eine entsprechende Zertifizierung durch eine IT-Sicherheits- oder Datenschutzüberprüfung (z.B. gemäß dem BSI Grundschutz) vorlegen.

4.3.3 Vor der Durchführung von Überprüfungen – einschließlich Inspektionen – prüft der Verantwortliche die vom Auftragsverarbeiter bereitgestellten Informationen ordnungsgemäß dahingehend, ob diese zum Nachweis der Einhaltung der in Artikel 28 DS-GVO niedergelegten Pflichten des Auftragsverarbeiters genügen. Der Verantwortliche führt Überprüfungen – einschließlich Inspektionen – nur durch, wenn der Verantwortliche die gut begründete Auffassung vertritt, dass die vom Auftragsverarbeiter bereitgestellten Informationen nicht ausreichend sind oder dass der Auftragsverarbeiter seine Pflichten aus Artikel 28 DS-GVO oder dieses Auftragsverarbeitungsvertrags verletzt.

4.3.4 Der Verantwortliche informiert den Auftragsverarbeiter rechtzeitig, mindestens zwei (2) Wochen im Voraus, über die Durchführung einer Überprüfung, einschließlich einer Inspektion.

4.3.5 Der Verantwortliche führt Inspektionen während der normalen Geschäftszeiten durch.

4.3.6 Das Betreten der Räumlichkeiten des Auftragsverarbeiters darf nur in ständiger Anwesenheit eines Vertreters des Auftragsverarbeiters erfolgen. Dieser Vertreter ist befugt, Entscheidungen über den Verlauf der Inspektion zu treffen, soweit dies erforderlich ist, um Störungen des Geschäftsbetriebs des Auftragsverarbeiters zu vermeiden und dessen Geheimhaltungspflichten gegenüber Dritten zu wahren.

4.3.7 Der Verantwortliche darf regelmäßige Überprüfungen – einschließlich Inspektionen – höchstens einmal pro Kalenderjahr durchführen. Der Verantwortliche darf zusätzliche Überprüfungen – einschließlich Inspektionen – nur aus einem von ihm nachzuweisenden wichtigen Grund durchführen.

4.3.8 Der Verantwortliche hat die Betriebs- und Geschäftsgeheimnisse des Auftragsverarbeiters, die dem Verantwortlichen während einer Überprüfung – einschließlich Inspektionen – bekannt werden, streng vertraulich zu behandeln. Der Verantwortliche erstellt keine Aufzeichnungen über diese Informationen, es sei denn, dies ist für die Ausübung seines Prüfungsrechts unbedingt erforderlich.

# 5. Pflichten des Auftragsverarbeiters

## 5.1 Verarbeitung auf dokumentierte Weisung des Verantwortlichen

5.1.1 Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten, die Gegenstand dieses Auftragsverarbeitungsvertrags sind, nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, zur

Verarbeitung verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

5.1.2 Der Auftragsverarbeiter stellt sicher, dass jede dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, die Gegenstand dieses Auftragsverarbeitungsvertrags sind, die Daten ausschließlich auf Weisung des Verantwortlichen verarbeitet, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet ist.

5.1.3 Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen die DS-GVO oder andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt. Der Auftragsverarbeiter ist befugt, die Ausführung der jeweiligen Weisung auszusetzen, bis sie vom Verantwortlichen bestätigt oder geändert wurde.

**5.2 Vertraulichkeit der Personen, die zur Verarbeitung der personenbezogenen Daten berechtigt sind**

5.2.1 Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten, die Gegenstand dieses Auftragsverarbeitungsvertrags sind, befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

**5.3 Sicherheit der Verarbeitung**

5.3.1 Der Auftragsverarbeiter ergreift alle gemäß Artikel 32 DS-GVO erforderlichen Maßnahmen.

5.3.2 Die konkreten vom Auftragsverarbeiter zu ergreifenden Maßnahmen sind in Anhang 2 dieses Auftragsverarbeitungsvertrags festgelegt.

5.3.3 Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Der Auftragsverarbeiter ist daher befugt, zusätzliche oder alternative Maßnahmen zu den in Anhang 2 dieses Auftragsverarbeitungsvertrags aufgeführten Maßnahmen zu ergreifen, solange das Sicherheitsniveau der bis dahin festgelegten Maßnahmen nicht unterschritten wird.

5.3.4 Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten, die Gegenstand dieses Auftragsverarbeitungsvertrags sind, bekannt wird, meldet er diese dem Verantwortlichen unverzüglich.

5.3.5 Der Verantwortliche trägt die ihm für die Erfüllung seiner Verpflichtungen aus einer Verletzung des Schutzes personenbezogener Daten entstandenen Kosten sowie die dem Auftragsverarbeiter für die Unterstützung des Verantwortlichen entstandenen angemessenen Kosten, es sei denn, die Verletzung des Schutzes personenbezogener

Daten beruht auf einem schuldhaften Verstoß des Auftragsverarbeiters gegen diesen Auftragsverarbeitungsvertrag oder Weisungen des Verantwortlichen.

**5.4 Beauftragung eines weiteren Auftragsverarbeiters**

5.4.1 Der Auftragsverarbeiter hält die folgenden in Artikel 28 (2) und (4) DS-GVO genannten Bedingungen für die Beauftragung eines weiteren Auftragsverarbeiters ein:

a) Der Auftragsverarbeiter informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

b) Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags dieselben Datenschutzpflichten auferlegt, wie sie in diesem Auftragsverarbeitungsvertrag festgelegt sind, 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 DS-GVO erfolgt.

c) Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.

5.4.2 Der Auftraggeber erteilt hiermit seine allgemeine Genehmigung, Unterauftragsverarbeiter unter den in 5.4.1 genannten Bedingungen zu beauftragen.

5.4.3 Ein Widerspruch des Verantwortlichen gegen eine beabsichtigte Änderung hinsichtlich der Hinzuziehung oder der Ersetzung von weiteren Auftragsverarbeitern ist nur zulässig, wenn dem Auftragnehmer ein wichtiger Grund nachgewiesen wird. Ein wichtiger Grund liegt nur vor, wenn die Änderung für den Verantwortlichen unter Berücksichtigung aller Umstände und unter Abwägung der Interessen beider Seiten nicht zumutbar ist. Der Verantwortliche kann nur innerhalb einer Frist von zwei (2) Wochen, nachdem er vom Auftragsverarbeiter über die Änderung informiert wurde, in Textform Widerspruch einlegen. Im Falle eines zulässigen Widerspruchs liegt es im Ermessen des Auftragsverarbeiters

a) die Verarbeitung ohne die geplante Änderung selbst oder über einen vom Auftragsverarbeiter mit der Genehmigung des Verantwortlichen beauftragten weiteren Auftragsverarbeiter weiterzuführen oder

b) alle Maßnahmen zu ergreifen, um den vom Verantwortlichen geltend gemachten Widerspruchsgrund zu beseitigen, den Verantwortlichen darüber zu informieren und erneut ein entsprechendes Widerspruchsrecht einzuräumen sowie die Verarbeitung mit der geplanten Änderung fortzusetzen, wenn entweder (i) die neue Widerspruchsfrist ohne einen erneuten Widerspruch des Verantwortlichen abgelaufen ist oder (ii) der Auftragsverarbeiter lediglich die vom Verantwortlichen

vorgeschlagenen Maßnahmen umgesetzt hat. Liegt ein zulässiger Widerspruchsgrund vor und ergreift der Auftragnehmer keine Maßnahmen zur Behebung des Widerspruchsgrunds, wird dem Verantwortlichen im Zeitraum von 14 Tagen nach Fristende die Möglichkeit einer Sonderkündigung des Vertragsverhältnisses eingeräumt.

5.5 **Unterstützung des Verantwortlichen bei der Erfüllung seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Rechte des Betroffenen**

5.5.1 Der Auftragsverarbeiter unterstützt den Verantwortlichen angesichts der Art der Verarbeitung mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DS-GVO genannten Rechte der betroffenen Personen nachzukommen.

**5.6 Unterstützung des Verantwortlichen bei der Einhaltung seiner Pflichten hinsichtlich der Sicherheit der Verarbeitung, der Dokumentation, der Meldung und Benachrichtigung von Verletzungen des Schutzes personenbezogener Daten, Datenschutz-Folgenabschätzung und vorheriger Konsultationen**

5.6.1 Unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Einhaltung der in den Artikel 32 bis 36 DS-GVO genannten Pflichten bezüglich personenbezogener Daten, die Gegenstand dieses Auftragsverarbeitungsvertrags sind.

**5.7 Löschung oder Rückgabe der personenbezogenen Daten an den Verantwortlichen nach Abschluss der Erbringung der Verarbeitungsleistungen**

5.7.1 Nach Abschluss der Erbringung der Dienstleistungen löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen entweder alle personenbezogenen Daten, die Gegenstand dieses Auftragsverarbeitungsvertrags sind, oder gibt diese an den Verantwortlichen zurück und löscht die vorhandenen Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

**5.8 Die Einrede des Zurückhaltungsrechts i.S.v. § 273 BGB wird hinsichtlich der verarbeiteten Daten ausgeschlossen.**

# 6. Übermittlung personenbezogener Daten an Drittländer

6.1 Vor Verlagerung der Verarbeitung in ein Drittland informiert der Auftragnehmer den Auftraggeber in Textform (bspw. per E-Mail). Der Auftraggeber kann der Änderung innerhalb von 3 Wochen ab Erhalt der Information durch den Auftragnehmer in schriftlicher Form oder in Textform (bspw. per E-Mail) begründet widersprechen. Erfolgt kein Widerspruch innerhalb der Frist, gilt die Zustimmung zur Änderung als

gegeben. Die Verlagerung der Verarbeitung in ein Drittland darf nur erfolgen, wenn die besonderen Voraussetzungen für die Übermittlung in ein Drittland nach Art. 44 ff. DS-GVO erfüllt sind.

# 7. Haftung

Die Haftung der Parteien richtet sich nach den anwendbaren gesetzlichen Regelungen.

# 8. Freistellung

Die Parteien erklären sich damit einverstanden, dass, wenn der Auftragnehmer für einen Verstoß gegen die Klauseln haftbar gemacht wird, den der Auftraggeber begangen hat, der Auftraggeber dem Auftragnehmer alle Kosten, Schäden, Ausgaben und Verluste, die dem Auftragnehmer entstanden sind, in dem Umfang ersetzt, in dem der Auftraggeber haftbar ist. Die Entschädigung ist abhängig davon, dass (a) der Auftragnehmer den Auftraggeber unverzüglich von einem Schadensersatzanspruch in Kenntnis setzt und (b) der Auftraggeber die Möglichkeit hat, mit dem Auftragnehmer bei der Verteidigung in der Schadensersatzsache bzw. der Einigung über die Höhe des Schadensersatzes zusammenzuarbeiten.

# 9. Laufzeit und Beendigung

Dieser Auftragsverarbeitungsvertrag tritt mit der Unterzeichnung durch beide Parteien in Kraft. Die Laufzeit dieses Auftragsverarbeitungsvertrags entspricht der Laufzeit des Hauptvertrags.

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

# 10. Anwendbares Recht und Gerichtsstand

10.1 Dieser Auftragsverarbeitungsvertrag unterliegt deutschem Recht.

10.2 Für alle Streitigkeiten, die im Zusammenhang mit diesem Auftragsverarbeitungsvertrag stehen, ist der ausschließliche Gerichtsstand, der Gerichtsstand der Hauptniederlassung des Auftragnehmers.

## 11. Schlussbestimmungen

11.1 Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er der Ansicht ist, dass dieser Auftragsverarbeitungsvertrag nicht den Anforderungen der einschlägigen Bestimmungen der DS-GVO und/oder etwaiger Richtlinien, Empfehlungen oder sonstiger Positionen der Aufsichtsbehörden, insbesondere des Europäischen Datenschutzausschusses (EDSA), an einen Auftragsverarbeitungsvertrag entspricht. In diesem Fall bemühen sich der Auftraggeber und der Auftragnehmer, diesen Auftragsverarbeitungsvertrag an die gesetzlichen und/oder behördlichen Anforderungen anzupassen.

11.2 Änderungen und Ergänzungen dieses Auftragsverarbeitungsvertrags bedürfen der Schriftform. Dies gilt auch für den Verzicht auf das Schriftformerfordernis.

11.3 Sollte eine Regelung dieses Auftragsverarbeitungsvertrags ganz oder teilweise unwirksam oder nicht durchsetzbar sein oder werden, berührt dies nicht die Gültigkeit der übrigen Regelungen. Die Parteien verpflichten sich, die unwirksame oder nicht durchsetzbare Regelung gemeinsam durch eine wirksame Regelung zu ersetzen, die der unwirksamen oder nicht durchsetzbaren Regelung soweit dies möglich ist entspricht. Gleiches gilt für jegliche Regelungslücken dieses Auftragsverarbeitungsvertrags.

11.4 Bei Widersprüchen zwischen diesem Auftragsverarbeitungsvertrag und anderen zwischen den Parteien geschlossenen Vereinbarungen, insbesondere dem Hauptvertrag, haben die Regelungen dieses Auftragsverarbeitungsvertrags Vorrang.

_____

Ort, Datum, Heyflow GmbH

_____

Ort, Datum, Unterschrift Auftraggeber

# Anhänge:

**Anhang 1:** Einzelheiten zur Verarbeitung

**Anhang 2:** Technische und organisatorische Maßnahmen des Auftragverarbeiters

**Anhang 3:** Unterauftragsverarbeiter der Endnutzerdaten

**Anhang 4:** Kontaktdaten Datenschutzbeauftragter

# **Anhang 1**: Einzelheiten zur Verarbeitung

| | |
|---|---|
| **Gegenstand der Verarbeitung** | Der Gegenstand der Verarbeitung ist die Erbringung der Dienstleistungen durch den Auftragnehmer. Der Auftragnehmer entwickelt Software zur Erstellung und Bereitstellung interaktiver Flows, die vom Auftraggeber beispielsweise zur Kundenbetreuung oder zur Gewinnung von Kunden oder Mitarbeitenden genutzt werden kann. |
| **Dauer der Verarbeitung** | Die Dauer der Verarbeitung ist durch die Dauer der Erbringung der Dienstleistungen bestimmt und endet mit Löschung des bei Heyflow erstellten Kundenkontos. |
| **Art und Zweck der Verarbeitung** | Der Auftragnehmer stellt dem Auftraggeber einen Software-Baukasten zur Erstellung von Flows zur Verfügung. Bei einem Flow handelt es sich um ein web-basiertes, interaktives Anfrageformular, das Kundenpräferenzen und/oder das Interesse von Kunden an bestimmten Produkten digital erfasst. Zudem ermöglicht der Auftragnehmer dem Auftraggeber über technische Schnittstellen, die vom Auftraggeber gestalteten Flows mit Services von Drittanbietern, beispielsweise Werbeplattformen oder Kundenmanagementsystemen, zu verknüpfen. Die Verknüpfung mit Services von Drittanbietern, auch solche, die über Heyflow bereitgestellt werden, wird durch entsprechende Einstellungen in der Heyflow App angewiesen und die damit zusammenhängende Datenverarbeitung vom Auftragnehmer entsprechend der Weisung ausgeführt. |
| **Art der personenbezogenen Daten** | Grundsätzlich hängt die Art der erhobenen Daten vom Einsatz des jeweiligen Baukastens und der Verwendung der durch den Baukasten zur Verfügung gestellten Eingabefelder ab. Daher kann die Art der erhobenen Daten durch den Auftragnehmer nicht pauschal eingegrenzt werden. Oftmals kommt es allerdings, bei entsprechender Veranlassung durch den Auftraggeber, zur Sammlung von personenbezogenen Daten wie beispielsweise Name, Adresse, E-Mail und Telefonnummer. Eine Erfassung der Daten erfolgt nur bei einer, durch den Endnutzer zu veranlassenden, Verwendung des sogenannten “Absenden-Buttons”. In diesem Kontext ist es möglich, über den Heyflow Baukasten eine entsprechende Zustimmungsfunktion zu integrieren. |
| **Betroffene Personen** | Wie beschrieben, können die betroffenen Personen durch den Auftragnehmer aufgrund des Baukastenprinzips pauschal nicht eingeschränkt werden. Im Regelfall werden jedoch Daten von potenziellen oder tatsächlichen Kaufinteressenten des Auftraggebers beziehungsweise von potenziellen oder tatsächlichen Mitarbeitenden gesammelt. |

# **Anhang 2:** Technische und organisatorische Maßnahmen des Auftragsverarbeiters

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Die technischen und organisatorischen Maßnahmen der Heyflow GmbH Gesamtorganisation sind ISO 27001 zertifiziert und werden in diesem Zuge regelmäßig intern und extern auditiert. Die hier beschriebenen Maßnahmen beziehen sich vorrangig auf Endnutzerdaten, also Informationen, die mithilfe von Heyflows Dienstleistungen und Produkten erhoben werden.

Der Auftragsverarbeiter, im Folgenden auch “wir”, “uns” oder “Heyflow”, erfüllt diesen Anspruch durch folgende Maßnahmen:

## 1. Vertraulichkeit gem. Art. 32 Abs. 1 lit. DS-GVO

**IT Infrastruktur**
Heyflow hat das Server-Hosting ihres Produktangebots an die führenden Cloud-Infrastruktur Anbieter ausgelagert. Google LLC (Google Cloud Platform) ist als einziger Unterauftragsverarbeiter mit der Verarbeitung und Speicherung von Endnutzerdaten beauftragt. Diese Lösung verspricht einen hohen Grad an physischer Sicherheit und Netzwerksicherheit. Die durch Heyflow angemieteten Server befinden sich ausschließlich in der Europäischen Union. Google Cloud Platform durchläuft regelmäßig strenge Sicherheitsaudits und ist unter anderem nach ISO 27001, ISO 27002, ISO 27017, ISO 27018 und SOC 2/3 zertifiziert. Die physischen, ökologischen und infrastrukturellen Sicherheitsvorkehrungen sind als Bestandteil der ISO 27001 und SOC 2 Typ 2 Zertifizierungen von unabhängigen Stellen bestätigt worden. Die entsprechenden Zertifikate sind unter https://cloud.google.com/security/compliance einsehbar.

**Interne Maßgaben**
Um die unbefugte Nutzung von Datenverarbeitungssystemen (Computern) zu verhindern werden des Weiteren mehrere Regeln berücksichtigt. Zunächst muss die Verwendung von starken Passwörtern gewährleistet sein. Darüber hinaus erfolgt jede Authentifizierung namensbezogen, Gruppen-Nutzer sind zu keinem Zeitpunkt erlaubt. Innerhalb des Unternehmens gelten außerdem die Regel der manuellen Desktopsperre, die alle Mitarbeitenden dazu auffordert ihren Computer manuell zu sperren, auch wenn der Arbeitsplatz nur kurzzeitig verlassen wird. Des Weiteren sind automatische Desktopsperren auf den Computern zu aktivieren, um im Falle einer ungeplanten Nicht-Anwesenheit eines Mitarbeitenden Missbrauch vorzubeugen. Jeder Computer kann nur über einen Zugang entsperrt werden. Hierbei müssen Benutzername und Passwort übereinstimmen.

Alle Computer verfügen über aktuellste Betriebssoftware, die mit jedem Update unverzüglich aktualisiert wird. Um dieser Anforderung nachzukommen, nutzt Heyflow eine virtuelle Fernverwaltung von Geräten der Mitarbeitenden. Hiermit wird sichergestellt, dass alle Computer, die sich innerhalb des Unternehmens in Gebrauch befinden, auf dem neuesten technischen Stand sind. Bei Nutzung eines Netzwerkes, das nicht von Heyflow kontrolliert wird, nutzen alle

Mitarbeitende ein virtuelles privates Netzwerk (VPN), das eine sichere Verbindung und Übertragung von Daten garantiert.

**Rollenkonzept**
Heyflow folgt einem zertifizierten Rollenkonzept bei der Verwaltung von Berechtigungen innerhalb des Unternehmens. Durch das Rollenkonzept wird die Nutzung je Benutzer und Ressource eindeutig nachvollziehbar. Jeder Rolle ist eine Vertretung zugeordnet, um Ausfälle zu vermeiden. Das Rollenkonzept soll insbesondere im Hinblick auf personelles Wachstum innerhalb des Unternehmens Geschäftsprozesse, Verantwortlichkeiten und Befugnisse eindeutig nachvollziehbar machen.

**Protokollierung**
Jegliche Aktivitäten in der Cloud-Infrastruktur werden innerhalb der entsprechenden Anwendung protokolliert, insbesondere bei der Eingabe, Änderungen und Löschung von Daten. Aktivitäten können einem Mitarbeitenden zugeordnet und eindeutig nachvollzogen werden.

**Trennungskontrolle**
Die Trennungskontrolle wird bei Heyflow durch die Anwendung des Rollenkonzepts gewährleistet. Weiterhin werden die durch Heyflow zur Verfügung gestellten Dienste in separaten virtuellen Ordnern bereitgestellt, sodass eine logische Trennung der Systeme gewährleistet werden kann. Abhängig vom gewählten Dienst werden die Anwendungen auch als dedizierte Anwendungen (als Google Cloud Platform Projekte) bereitgestellt, wodurch eine erhöhte zweckmäßige Trennung der Datenverarbeitung gewährleistet werden kann.

## 2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

**Datenweitergabe und -speicherung**
Zur Weitergabekontrolle findet innerhalb des Unternehmens das Rollenkonzept Anwendung. Grundsätzlich werden innerhalb des Unternehmens keine personenbezogenen Daten von Endnutzern weitergeben. In begründeten Ausnahmefällen werden Daten protokolliert übergeben und schnellstmöglich gelöscht. Niemals werden Daten an Dritte ohne die schriftliche Aufforderung/Einverständnis des Kunden weitergegeben.

Die Weitergabe der Endnutzerdaten an den Kunden ist verschlüsselt. Dies beinhaltet die Weitergabe von Daten per E-Mail mit einem gültigen TLS/SSL Zertifikat (TLS Version 1.0 und höher) via SMTP. Jegliche Daten, die über die von Heyflow zur Verfügung gestellten Dienste versendet werden (“In Transit”), sind mit einem SHA-256 (mit RSA-Verschlüsselung) TLS (Version 1.1 und aufwärts) Zertifikat verschlüsselt. Jegliche von Heyflow gespeicherten Daten (“At Rest”), sind mit dem Advanced Encryption Standard (AES) Algorithmus, AES-256, verschlüsselt. Im Detail verwenden wir und die relevanten Unterauftragsverarbeiter die kryptografische Bibliothek Tink mit FIPS 140-2-Validierung, um die Verschlüsselung zu garantieren.

Grundsätzlich werden keine personenbezogenen Daten an Heyflow und ihre Unterauftragsverarbeiter gesendet, bevor der Endnutzer nicht über einen “Absenden”-Button, der als Teil des Heyflow Baukastens verfügbar ist, seine Daten absendet.

Beim Aufruf eines Heyflows sowie bei Navigation innerhalb eines Heyflows, werden nicht-personenbezogene Informationen an Heyflow gesendet, die für die Verarbeitung von

Verhaltensdaten, die im *Analytics Dashboard* innerhalb der Heyflow Applikation angezeigt werden, notwendig sind. Diese Informationen sind beispielsweise die Identifikationsnummer des Heyflows (Heyflow ID), die aufgerufene URL, die Bildschirmgröße und die Kennung des Browsers. Die IP-Adresse des Endnutzers wird ausdrücklich nicht verarbeitet und gespeichert.

Neben der Speicherung von Endnutzerantworten innerhalb des Systems, bietet Heyflow Schnittstellen zu externen Anbietern und Programmen an, z.B. Slack, HubSpot, und Salesforce, an die Endnutzerdaten gesendet werden, sofern der Heyflow Nutzer dies explizit konfiguriert und aktiviert hat. Heyflow versendet die Endnutzerdaten zu jeder Zeit über sichere Verbindungen (HTTPS/TLS), kann jedoch nicht für die Verarbeitung und Speicherung der Daten innerhalb der Fremdsysteme verantwortlich sein.

Innerhalb des Unternehmens werden keine mobilen Speichermedien (USB-Sticks etc.) verwendet.

**Softwareentwicklung und -veränderungen**
Programmatische Änderungen an den von Heyflow zur Verfügung gestellten Dienste werden mittels der Versionierungstechnologie *git* protokolliert und können so nachvollzogen werden. Hierzu muss sich der verantwortliche Entwickler eindeutig authentifizieren und vorab für die entsprechenden Änderungen registriert worden sein. Aktivitäten innerhalb der Cloud-Infrastruktur werden protokolliert und können nachvollzogen werden (siehe 1).

**Ändern und Löschen von Endnutzerdaten**
Endnutzerdaten werden automatisiert und verschlüsselt über eigens dafür entwickelte Software-Systeme verarbeitet. Dem Endnutzer ist es nicht möglich über diese Schnittstelle seine versendeten Daten zu ändern oder zu löschen. Berechtigte Mitarbeitende von Heyflow haben Zugriff auf die Cloud-Infrastruktur über welche Daten eingegeben, geändert und gelöscht werden können. Zur Eingabekontrolle findet innerhalb von Heyflow das Rollenkonzept Anwendung nach diesem Rechte zur Eingabe, Änderung und Löschen von Daten vergeben werden.

**Datenschutzrelevante Zusatzfunktionen des Heyflow Baukastens**
Heyflow bietet die Funktionalität an, sensible Fragen als solche zu kennzeichnen, wodurch diese nur für Weitergabe an den Kunden verarbeitet werden und darüber hinaus nicht im Heyflow-System gespeichert werden („Sensitive-Tag”). Heyflow empfiehlt grundsätzlich allen Kunden, von dieser Funktionalität bei personenbezogenen Daten Gebrauch zu machen.

Eine weitere Funktionalität, die es unseren Kunden erleichtert, Datenschutzkonform zu sein, ist die automatische Löschung von veralteten Endnutzerantworten. Heyflow Nutzer finden diese Funktion in den Einstellungen ihres Heyflows.

Bei Verwendung der *Wiederherstellen* Funktion, die die Eingaben der Endnutzer über Folgebesuche persistiert wird zusätzlich ein Feld im sog. localStorage angelegt, in dem die Eingaben im Browser des Endnutzers gespeichert werden. Ähnlich wird bei Verwendung von Heyflows Cookie-Zustimmungsverwalter ein Feld im localStorage angelegt, der die Privatsphäreneinstellung des Endnutzers über Folgebesuche speichert.

## 3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Heyflow hat das Server-Hosting ihres Produktangebots an die führenden Cloud-Infrastruktur Anbieter ausgelagert. Oben genannte Anbieter durchlaufen regelmäßig strenge Sicherheitsaudits und sind unter anderem nach ISO 27001, ISO 27002, ISO 27017, ISO 27018 und SOC 2/3 zertifiziert.

## 4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Mitarbeitende werden regelmäßig (halbjährlich) zum Datenschutz sensibilisiert und auf Vertraulichkeit verpflichtet. Eine Datenschutz-Folgenabschätzung wird bei Bedarf und in enger Absprache mit Verantwortlichen durchgeführt. Heyflow Nutzer und Endnutzer finden den formalisierten Prozess zu Auskunftsanfragen in unserer Datenschutzerklärung. Wir haben alle Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für alle Mitarbeitende nach Bedarf bzw. Berechtigung zur Verfügung gestellt. Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird darüber hinaus unter Aufsicht des Leiters der IT halbjährlich durchgeführt.

Kritische Sicherheitsvorfälle und Datenpannen werden via Ticketsystem dokumentiert und umgehend unseren Kunden telefonisch oder per E-Mail mitgeteilt. Eine gegebenenfalls vorliegende Meldepflicht gegenüber Aufsichtsbehörden wird nachgekommen.

Wir folgen dem „Privacy by default”-Konzept und erheben nur die personenbezogenen Daten, die für die Nutzung unserer Dienste notwendig sind.

Alle Unterauftragsverarbeiter werden von uns im Vorfeld im Hinblick auf die implementierten Sicherheitsmaßnahmen und deren Dokumentation überprüft. Die Auswahl der Unterauftragsverarbeiters findet unter Sorgfaltsgesichtspunkten (insbesondere in Bezug auf Datenschutz und Datensicherheit) statt. Ein Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standardvertragsklauseln ist zwingend.

# **Anhang 3:** Unterauftragsverarbeiter von Endnutzerdaten

| **Name und Adresse des Unterauftrags-verarbeiters** | **Umfang, Art und Zweck der Unter-auftragsver-arbeitung** | **Kategorien der betroffenen Personen** | **Kategorien der personenbezogen-en Daten** | **Dauer der Unterauftrags-verarbeitung** | **Ort der Unter-auftragsver-arbeitung** |
|---|---|---|---|---|---|
| Google Ireland Limited<br>Gordon House, Barrow Street<br>Dublin 4<br>Ireland | Google Cloud Platform zur Bereitstellung und Betrieb der Server. | Kunden, Endnutzer | Durch den Auftraggeber mittels Heyflow erhobene Daten | Unbestimmt | Europäische Union |
| Amazon Web Services EMEA SARL<br><br>38 Avenue John F. Kennedy, L-1855, Luxembourg | Versand von Anfragedaten per E-Mail an Auftraggeber | Kunden, Endnutzer | Durch den Auftraggeber mittels Heyflow erhobene Daten, sofern die Funktion zum automatischen Email Versand aktiviert ist | Unbestimmt | Germany |
| Tinybird, Inc<br><br>41 East 11th Street, 11th Floor, New York, NY 10003, USA | Echtzeit-Datenverar beitung zur Verbesserung der Abfrage und Visualisierung von Datenflussanalysen | Kunden, Endnutzer | Durch den Auftraggeber mittels Heyflow erhobene Daten | Unbestimmt | EU |

# **Anhang 4:** Kontaktdaten Datenschutzbeauftragter

Heyflow vertraut auf die Dienste des externen Datenschutzdienstleisters Proliance GmbH.

Kontaktdaten:

PROLIANCE GmbH
Dominik Fürkner
www.datenschutzexperte.de
Leopoldstr. 21
80802 München
datenschutzbeauftragter@datenschutzexperte.de