Bestimmungen zur Auftragsverarbeitung

Präambel

Die Parteien haben einen Vertrag geschlossen, nach dem Heyflow dem Kunden bestimmte Dienstleistungen bereitstellt.

Bei der Erbringung dieser Dienstleistungen kann Heyflow als Auftragsverarbeiter im Sinne von Art. 4 Nr. 8 DSGVO personenbezogene Daten im Sinne von Art. 4 Nr. 1 DSGVO im Auftrag des Kunden als Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO verarbeiten.

Verweise auf die DSGVO in dieser Vereinbarung zur Auftragsverarbeitung (AVV) umfassen, soweit zutreffend, auch die britische DSGVO („UK GDPR“) gemäß der „Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019“ sowie das britische Datenschutzgesetz 2018 („UK Data Protection Act 2018“).

1. Definitionen

1.1 **Für die Zwecke dieser Bestimmungen zur Auftragsverarbeitung finden die Begriffsbestimmungen des Artikel 4 DSGVO Anwendung, sofern nachfolgend nicht etwas anderes bestimmt ist.**

1.2 **Für die Zwecke dieser Bestimmungen zur Auftragsverarbeitung finden die folgenden abweichenden und/oder zusätzlichen Begriffsbestimmungen Anwendung:**

1.2.1 Ein „Flow” ist ein web-basiertes, interaktives Anfrageformular, das über den von Heyflow angebotenen Software-Baukasten durch den Kunden eigenverantwortlich konfiguriert werden kann.

1.2.2 „Endnutzer” meint denjenigen Nutzer, der den vom Kunden eingesetzten Flow nutzt.

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

1.2.4 „EWR” ist der Europäische Wirtschaftsraum.

1.2.5 „Drittland” ist jedes Land außerhalb des EWR.

1.2.6 „Hauptvertrag” ist der zwischen den Parteien abgeschlossene Leistungsvertrag einschließlich Heyflows Allgemeiner 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 Kunde und Heyflow.

1.2.9 „Services" und Dienste sind die von Heyflow für den Kunden im Rahmen des Hauptvertrages zu erbringenden Leistungen, wie in den Allgemeinen Geschäftsbedingungen und etwaigen zusätzlichen Vertragsabreden beschrieben.

1.2.10 „Sichere Drittländer" sind alle Drittländer, für die ein Angemessenheitsbeschluss der Europäischen Kommission gemäß Artikel 45 (3) DSGVO 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) DSGVO in Anspruch nimmt.

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

1.2.14 „CCPA" bezeichnet den California Consumer Privacy Act (Kalifornisches Verbraucherdatenschutzgesetz), einschließlich aller Änderungen und zugehöriger Durchführungsbestimmungen. Dieses Gesetz (a) gewährt Einwohnern Kaliforniens bestimmte Rechte in Bezug auf ihre personenbezogenen Daten, (b) verpflichtet Unternehmen, die solche Daten erheben, verwenden oder weitergeben, zu bestimmten Maßnahmen, und (c) gibt Verbrauchern das Recht, auf ihre Daten zuzugreifen, deren Löschung zu verlangen oder dem Verkauf ihrer personenbezogenen Daten zu widersprechen.

2. Anwendungsbereich, Parteien und ihre jeweiligen Rollen

2.1 Diese Bestimmungen zur Auftragsverarbeitung finden Anwendung auf die Verarbeitung personenbezogener Daten durch Heyflow bei der Erbringung der Services.

2.2 Heyflow stellt dem Kunden einen Software-Baukasten zur Erstellung von Flows zur Verfügung. Grundsätzlich obliegt die Ausgestaltung der Flows durch die Verwendung des Baukastens dem Kunden. Heyflow kann die Art der durch einen Flow erhobenen Daten nicht pauschal eingrenzen. Heyflow stellt dem Kunden eine optional zu

verwendende Produktfunktionalität zur Verfügung, die die Speicherung von personenbezogenen Daten von Endnutzern durch Heyflow verhindert. Die sachgemäße Verwendung der entsprechenden Funktion obliegt dem Kunden.

2.3 Bei Widersprüchen zwischen diesen Bestimmungen zur Auftragsverarbeitung und zwischen den von den Parteien geschlossenen Vereinbarungen, insbesondere dem Hauptvertrag, haben die Regelungen dieser Bestimmungen zur Auftragsverarbeitung Vorrang.

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 dieser Bestimmungen zur Auftragsverarbeitung festgelegt.

4. Rechte des Kunden

4.1 Weisungsrecht

4.1.1 Der Kunde hat das Recht, Weisungen an Heyflow bezüglich der Verarbeitung personenbezogener Daten nach diesen Bestimmungen zur Auftragsverarbeitung zu erteilen.

4.1.2 Diese Bestimmungen, insbesondere die Bestimmung der Details der Verarbeitung gemäß Abschnitt 3, verstehen sich als allgemeine Weisungen, personenbezogene Daten so zu verarbeiten, wie es für die Erbringung der Services vernünftigerweise erforderlich ist und mit diesen Bestimmungen und dem Hauptvertrag vereinbart ist.

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

4.2 Recht auf Auskunft und auf Durchführung von Überprüfungen, einschließlich Inspektionen

4.2.1 Der Kunde hat das Recht, von Heyflow alle erforderlichen Informationen zum Nachweis der Einhaltung der in Artikel 28 DSGVO niedergelegten Pflichten zu verlangen.

4.2.2 Zum Nachweis der Einhaltung seiner Pflichten kann Heyflow 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.

4.2.3 Ist der Kunde nach ordnungsgemäßer Prüfung der von Heyflow bereitgestellten Informationen dahingehend, ob diese zum Nachweis der Einhaltung der in Artikel 28 DSGVO niedergelegten Pflichten genügen, der gut begründeten Auffassung, dass die bereitgestellten Informationen nicht ausreichend sind oder dass Heyflow seine Pflichten aus Artikel 28 DSGVO oder dieser Bestimmungen zur Auftragsverarbeitung verletzt, hat er das Recht, Überprüfungen – einschließlich Inspektionen – bei Heyflow entweder selbst oder durch einen von ihm beauftragten Prüfer durchzuführen.

4.2.4 Die Durchführung von Überprüfungen und/oder Inspektionen, die der Kunde Heyflow nicht rechtzeitig, mindestens zwei (2) Wochen im Voraus, angekündigt, darf Heyflow verweigern.

4.2.5 Inspektionen außerhalb der normalen Geschäftszeiten darf Heyflow verweigern.

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

4.2.7 Heyflow duldet die Durchführung regelmäßiger Überprüfungen – einschließlich Inspektionen – höchstens einmal pro Kalenderjahr. Zusätzliche Überprüfungen – einschließlich Inspektionen – duldet Heyflow nur im Falle eines vom Kunden nachzuweisenden wichtigen Grund..

4.2.8 Die hier geregelten Überprüfungs- und Inspektionsrechte stehen unter dem Vorbehalt, dass der Kunde die Betriebs- und Geschäftsgeheimnisse Heyflows, die dem Kunden während einer Überprüfung – einschließlich Inspektionen – bekannt werden, streng vertraulich behandelt. Heyflow gestattet es dem Kunden nicht, Aufzeichnungen über Betriebs- und Geschäftsgeheimnisse Heyflows, die dem Kunden während einer Überprüfung – einschließlich Inspektionen – bekannt werden, aufzuzeichnen, es sei denn, dies ist für die Ausübung des Prüfungsrechts unbedingt erforderlich.

5. Pflichten Heyflows

5.1 Verarbeitung auf dokumentierte Weisung des Kunden

5.1.1 Heyflow verarbeitet die personenbezogenen Daten, die Gegenstand der Auftragsverarbeitung sind, nur auf dokumentierte Weisung des Kunden – 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 Heyflow unterliegt, zur Verarbeitung verpflichtet ist; in einem solchen Fall teilt Heyflow dem Kunden diese rechtlichen Anforderungen vor der

Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

5.1.2 Heyflow stellt sicher, dass jede Heyflow unterstellte Person, die Zugang zu personenbezogenen Daten hat, die Gegenstand dieser Bestimmungen zur Auftragsverarbeitung sind, die Daten ausschließlich auf Weisung des Kunden verarbeitet, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet ist.

5.1.3 Der Kunde informiert Heyflow unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen die DSGVO oder andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt. Heyflow ist befugt, die Ausführung der jeweiligen Weisung auszusetzen, bis sie vom Kunden bestätigt oder geändert wurde.

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

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

5.3 Sicherheit der Verarbeitung

5.3.1 Heyflow ergreift alle gemäß Artikel 32 DSGVO erforderlichen Maßnahmen.

5.3.2 Die konkreten von Heyflow zu ergreifenden Maßnahmen sind in Anhang 2 dieser Bestimmungen zur Auftragsverarbeitung festgelegt.

5.3.3 Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Heyflow ist daher befugt, zusätzliche oder alternative Maßnahmen zu den in Anhang 2 dieser Bestimmungen zur Auftragsverarbeitung aufgeführten Maßnahmen zu ergreifen, solange das Sicherheitsniveau der bis dahin festgelegten Maßnahmen nicht unterschritten wird.

5.3.4 Wenn Heyflow eine Verletzung des Schutzes personenbezogener Daten, die Gegenstand der Auftragsverarbeitung sind, bekannt wird, meldet Heyflow diese dem Kunden unverzüglich.

5.3.5 Heyflow trägt keine Kosten, die dem Kunden für die Erfüllung seiner Verpflichtungen aus einer Verletzung des Schutzes personenbezogener Daten entstanden sind und behält sich vor, dem Kunden die für die Unterstützung entstandenen angemessenen Kosten in Rechnung zu stellen, es sei denn, die Verletzung des Schutzes personenbezogener Daten beruht auf einem schuldhaften Verstoß Heyflows gegen Heyflows Pflichten nach diesen Bestimmungen zur Auftragsverarbeitung oder gegen Weisungen des Kunden.

5.4 Beauftragung weiterer Auftragsverarbeiter

5.4.1 Heyflow hält die folgenden in Artikel 28 (2) und (4) DSGVO genannten Bedingungen für die Beauftragung eines weiteren Auftragsverarbeiters ein:

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

b) Nimmt Heyflow die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten für den Kunden auszuführen, so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags oder eines anderes Rechtsinstruments im Sinne des Art. 28 DSGVO dieselben Datenschutzpflichten auferlegt, wie sie in diesen Bestimmungen zur Auftragsverarbeitung 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 DSGVO erfolgt.

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

5.4.2 Heyflow nimmt bei der Auftragsverarbeitung die Dienste der in Anhang 3 dieser Bestimmungen zur Auftragsverarbeitung genannten weiteren Auftragsverarbeiter in Anspruch.

5.4.3 Weist der Kunde Heyflow nach, dass eine beabsichtigte Änderung hinsichtlich der Hinzuziehung oder der Ersetzung von weiteren Auftragsverarbeitern für den Kunden unter Berücksichtigung aller Umstände und unter Abwägung der Interessen beider Seiten nicht zumutbar ist und legt deshalb innerhalb einer Frist von zwei (2) Wochen, nachdem er von Heyflow über die Änderung informiert wurde, in Textform Widerspruch ein, liegt es im Ermessen Heyflows

a) die Verarbeitung ohne die geplante Änderung selbst oder über einen von Heyflow mit der Genehmigung des Kunden beauftragten weiteren Auftragsverarbeiter weiterzuführen oder

b) alle Maßnahmen zu ergreifen, um den vom Kunden geltend gemachten Widerspruchsgrund zu beseitigen, den Kunden 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 Kunden abgelaufen ist oder (ii) Heyflow lediglich die vom Kunden vorgeschlagenen Maßnahmen umgesetzt hat. Liegt ein zulässiger Widerspruchsgrund vor und ergreift Heyflow keine Maßnahmen zur Behebung des Widerspruchsgrunds, wird dem Kunden im Zeitraum von 14 Tagen nach Fristende die Möglichkeit einer Sonderkündigung des Vertragsverhältnisses eingeräumt.

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

5.5.1 Heyflow unterstützt den Kunden angesichts der Art der Verarbeitung mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DSGVO genannten Rechte der betroffenen Personen nachzukommen.

5.6 Unterstützung des Kunden 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 Heyflow zur Verfügung stehenden Informationen unterstützt Heyflow den Kunden bei der Einhaltung der in den Artikel 32 bis 36 DSGVO genannten Pflichten bezüglich personenbezogener Daten, die Gegenstand der Auftragsverarbeitung sind.

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

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

6. Übermittlung personenbezogener Daten an Drittländer

6.1 Vor Verlagerung der Verarbeitung in ein Drittland informiert Heyflow den Kunden in Textform (bspw. per E-Mail). Der Kunde kann der Änderung innerhalb von 3 Wochen ab Erhalt der Information durch Heyflow in schriftlicher Form oder in Textform (bspw. per E-Mail) begründet widersprechen. Die Verlagerung der Verarbeitung in ein Drittland darf nur erfolgen, wenn die besonderen Voraussetzungen für die Übermittlung in ein Drittland nach Art. 44 ff. DSGVO erfüllt sind.

7. Haftung

Die Haftung Heyflows richtet sich nach den anwendbaren gesetzlichen Regelungen.

8. Laufzeit und Beendigung

Die Dauer der Auftragsverarbeitung richtet sich nach der Laufzeit des Hauptvertrages. Nach Ende des Hauptvertrages ist Heyflow gegenüber dem Kunden nicht mehr an diese Bestimmungen gebunden.

Anhänge:

Anhang 1: Einzelheiten zur Verarbeitung

Anhang 2: Technische und organisatorische Maßnahmen Heyflows

Anhang 3: Unterauftragsverarbeiter der Endnutzerdaten

Anhang 1: Einzelheiten der Verarbeitung

Gegenstand der Verarbeitung	Der Gegenstand der Verarbeitung ist die Erbringung der Dienstleistungen durch Heyflow. Heyflow entwickelt Software zur Erstellung und Bereitstellung interaktiver Flows, die vom Kunden 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	Heyflow stellt dem Kunden 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 Heyflow dem Kunden über technische Schnittstellen, die vom Kunden 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 von Heyflow entsprechend der Weisung des Kunden 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 Heyflow nicht pauschal eingegrenzt werden. Oftmals kommt es allerdings, bei entsprechender Veranlassung durch den Kunden, 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 Heyflow aufgrund des Baukastenprinzips pauschal nicht eingeschränkt werden. Im Regelfall werden jedoch Daten von potenziellen oder tatsächlichen Kaufinteressenten des Kunden beziehungsweise von potenziellen oder tatsächlichen Mitarbeitenden gesammelt.

Anhang 2: Technische und organisatorische Maßnahmen Heyflows

Organisationen, die personenbezogene Daten selbst oder im Auftrag verarbeiten oder nutzen, sind verpflichtet, die technischen und organisatorischen Maßnahmen zu ergreifen, die erforderlich sind, um die Vorschriften der Datenschutzgesetze umzusetzen. Maßnahmen sind nur insoweit erforderlich, als ihr wirtschaftlicher Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht.

Die technischen und organisatorischen Maßnahmen der Gesamtorganisation der Heyflow GmbH sind nach ISO 27001 zertifiziert und werden regelmäßig sowohl intern als auch extern geprüft. Heyflow stellt einen aktuellen Überblick über den jeweiligen Compliance-Status im öffentlich zugänglichen Heyflow Trust Center unter https://trust.heyflow.com/ bereit.

Die in diesem Dokument beschriebenen Maßnahmen beziehen sich vorrangig auf Endnutzerdaten, also Informationen, die durch die Nutzung der Dienste und Produkte von Heyflow erhoben werden.

Heyflow – nachfolgend auch als „wir“ oder „uns“ bezeichnet – erfüllt diese Anforderungen durch die folgenden Maßnahmen:

1. Vertraulichkeit gem. Art. 32 Abs. 1 lit. DSGVO

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 können unter folgendem Link eingesehen werden: https://cloud.google.com/security/compliance/compliance-reports-manager.

Interne Prozesse und Maßgaben
Um die unbefugte Nutzung von Datenverarbeitungssystemen (z. B. Computern) zu verhindern, werden mehrere Sicherheitsregeln berücksichtigt. Zunächst ist die Verwendung von starken Passwörtern zwingend vorgeschrieben. Darüber hinaus erfolgt jede Authentifizierung personenbezogen; die Nutzung von Gruppenbenutzern für Datenverarbeitungssysteme ist nicht gestattet.

Innerhalb des Unternehmens gilt die Regel zur manuellen Sperrung von Arbeitsplätzen: Alle Mitarbeitenden sind verpflichtet, ihren Computer manuell zu sperren, auch bei kurzer Abwesenheit

vom Arbeitsplatz. Zusätzlich müssen alle Computer so konfiguriert sein, dass sie sich nach einer gewissen Inaktivitätszeit automatisch sperren, um eine missbräuchliche Nutzung bei unerwarteter Abwesenheit zu verhindern. Jeder Computer kann nur über einen definierten Zugangspunkt entsperrt werden, wobei Benutzername und Passwort übereinstimmen müssen.

Alle Computer sind mit aktuellen Betriebssystemen ausgestattet und erhalten innerhalb von 14 Tagen nach Veröffentlichung von Software-Updates die entsprechenden Aktualisierungen. Zur Einhaltung dieser Anforderung nutzt Heyflow ein virtuelles Remote-Management der Endgeräte der Mitarbeitenden. Damit wird sichergestellt, dass alle im Unternehmen verwendeten Computer stets auf dem neuesten Stand der Technik sind.

Beim Zugriff auf kundensensitive Schnittstellen ist die Nutzung eines Virtual Private Network (VPN) für alle Mitarbeitenden verpflichtend, um eine sichere Verbindung und Datenübertragung zu gewährleisten.

Privilegierte Zugriffe auf Produktionsinfrastrukturen sind durch Multi-Faktor-Authentifizierung (MFA) abgesichert. Der Zugriff auf Systemprogramme und -werkzeuge ist ausschließlich autorisierter Fachperson vorbehalten. Passwörter werden gemäß interner Richtlinien ausschließlich in sicheren Passwort-Tresoren (z. B. 1Password, Google Passwords) gespeichert und geteilt.

Rollenkonzept
Heyflow verfolgt ein zertifiziertes Rollenkonzept zur Verwaltung von Berechtigungen innerhalb des Unternehmens. Das Rollenkonzept gewährleistet eine vollständige Nachvollziehbarkeit der Nutzung durch einzelne Benutzer und der Zuweisung von Ressourcen. Jeder Rolle ist eine Vertretung zugeordnet, um Ausfälle zu vermeiden. Ziel des Rollenkonzepts ist es, Geschäftsprozesse, Zuständigkeiten und Zugriffsrechte eindeutig nachvollziehbar zu gestalten – insbesondere im Hinblick auf das personelle Wachstum des Unternehmens.

Alle Mitarbeitenden durchlaufen einen strukturierten Onboarding-Prozess, der Schulungen und Qualifizierungen zu Datenschutz und IT-Sicherheit beinhaltet.

Die Einrichtung und Entziehung von Benutzerzugängen wird über ein internes System (CakeWalk) dokumentiert. Jede Berechtigung muss formell genehmigt werden. Zugriffsrechte, einschließlich solcher für privilegierte Nutzer und technische Servicekonten, werden mindestens einmal jährlich überprüft.

Die Entziehung von Zugriffsrechten (Deprovisionierung) hat spätestens innerhalb von 48 Geschäftsstunden nach Beendigung des Vertragsverhältnisses oder einer Rollenänderung zu erfolgen.

Trennungsgebot
Heyflow gewährleistet die Einhaltung des Trennungsgebots durch die Anwendung des unternehmensweit implementierten Rollenkonzepts. Darüber hinaus werden die von Heyflow bereitgestellten Dienste in separaten virtuellen Umgebungen (Ordnern) zur Verfügung gestellt, sodass eine logische Trennung der Systeme sichergestellt ist.

Abhängig vom jeweils gewählten Dienst werden Anwendungen zudem als dedizierte Applikationen innerhalb eigenständiger Google Cloud Platform-Projekte bereitgestellt. Dies trägt zusätzlich zu einer erhöhten Trennung der Datenverarbeitung und zur Vermeidung von ungewollten Zugriffen oder Datenvermischung bei.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Datenweitergabe und -speicherung
Zur Kontrolle der Datenübertragung wird unternehmensintern das Rollenkonzept angewendet. Grundsätzlich erfolgt keine Weitergabe personenbezogener Daten von Endnutzern innerhalb des Unternehmens. In begründeten Ausnahmefällen kann eine datenprotokollierte Weitergabe erfolgen; diese Daten werden jedoch so schnell wie möglich gelöscht. Eine Weitergabe an Dritte erfolgt ausschließlich auf schriftliche Anforderung.

Die Übermittlung von Endnutzerdaten an den Kunden erfolgt verschlüsselt. Dies umfasst auch die Übertragung per E-Mail mit einem gültigen TLS/SSL-Zertifikat (mindestens TLS-Version 1.1) über SMTP. Daten, die im Rahmen der Dienste von Heyflow übertragen werden („In Transit“), sind mit einem SHA-256-Zertifikat (mit RSA-Verschlüsselung) und TLS ab Version 1.1 gesichert. Gespeicherte Daten („At Rest“) werden mithilfe des Advanced Encryption Standard (AES) nach dem AES-256-Verfahren verschlüsselt.

Darüber hinaus sind die unternehmensweiten Verschlüsselungsrichtlinien an die jeweils aktuellen Empfehlungen des National Institute of Standards and Technology (NIST), insbesondere NIST SP 800-57, angelehnt. Vertrauliche Unternehmens- oder Kundendaten, unabhängig davon, ob sie sich in Übertragung oder in Speicherung befinden, werden unter Verwendung von Algorithmen wie AES-256 oder SCRYPT verschlüsselt – abhängig von ihrer Klassifizierung und dem jeweiligen Stadium ihres Datenlebenszyklus. Die Speicherung von Daten auf mobilen Datenträgern ist grundsätzlich untersagt, es sei denn, sie erfolgt verschlüsselt und wurde ausdrücklich genehmigt.

Grundsätzlich werden keine personenbezogenen Daten an Heyflow oder dessen Unterauftragsverarbeiter übermittelt, bevor der Endnutzer entweder aktiv seine Daten über die „Absenden“-Schaltfläche übermittelt oder eine Zahlung über den Stripe-Zahlungsblock initiiert. Beide Optionen stehen dem Kunden innerhalb der Heyflow-Anwendung zur Verfügung und sind dort konfigurierbar.

Beim Zugriff auf einen Heyflow und während der Navigation innerhalb eines Heyflows werden keine personenbezogenen Daten, sondern ausschließlich nicht-personenbezogene Informationen an Heyflow übertragen. Diese Informationen sind erforderlich für die Analyse des Nutzerverhaltens im Analytics-Dashboard der Heyflow-Anwendung sowie zur Fehlerverfolgung und technischen Nachvollziehbarkeit (Observability). Zu den übermittelten Daten zählen unter anderem: die Heyflow-ID, die aufgerufene URL, Bildschirmgröße, Browserkennung und Debug-Protokolle. Die IP-Adresse des Endnutzers wird ausdrücklich weder verarbeitet noch gespeichert.

Zusätzlich zur Speicherung der Endnutzerantworten im eigenen System bietet Heyflow Schnittstellen zu externen Diensten und Plattformen wie Slack, HubSpot oder Salesforce an. Eine Übertragung von Endnutzerdaten an diese Drittanbieter erfolgt nur, wenn der Kunde die jeweilige Integration explizit konfiguriert und aktiviert hat. Heyflow überträgt dabei sämtliche Daten

ausschließlich über sichere Verbindungen (HTTPS/TLS), übernimmt jedoch keine Verantwortung für die anschließende Verarbeitung oder Speicherung der Daten in den Drittsystemen.

Softwareentwicklung und -veränderungen
Programmgesteuerte Änderungen an den von Heyflow bereitgestellten Diensten werden mithilfe der Versionierungstechnologie Git protokolliert und sind dadurch vollständig nachvollziehbar. Für diesen Zweck muss der verantwortliche Entwickler eindeutig authentifiziert sein und vorab für die jeweiligen Änderungen registriert werden.

Aktivitäten innerhalb der Cloud-Infrastruktur werden ebenfalls protokolliert und sind nachverfolgbar (vgl. Abschnitt 1).

Die Codeentwicklung erfolgt nach einem sicheren, strukturierten Release-Prozess, der unter anderem folgende Stufen umfasst:

- Verwendung getrennter Umgebungen (Development, Staging, Production), Automatisierte Regressionstests,
- Peer Reviews (Vier-Augen-Prinzip),
- sowie manuelle Qualitätssicherungsprüfungen (QA) vor der Bereitstellung in die Produktivumgebung.

Die Entwickler:innen erhalten regelmäßig Schulungen zum sicheren Programmieren, insbesondere zur Vermeidung von Bedrohungen gemäß OWASP Top 10.

Zur weiteren Erhöhung der Sicherheit werden bei Heyflow jährlich Penetrationstests durchgeführt, um potenzielle Schwachstellen in der Anwendung zu identifizieren und zu beheben.

Änderung und Löschung von Endnutzerdaten
Die Verarbeitung von Endnutzerdaten erfolgt automatisiert und verschlüsselt mithilfe speziell entwickelter Softwaresysteme. Eine Änderung oder Löschung der übermittelten Daten durch den Endnutzer selbst über die Benutzeroberfläche ist nicht möglich.
Autorisierte Mitarbeitende von Heyflow haben Zugriff auf die Cloud-Infrastruktur, über die Daten eingegeben, geändert und gelöscht werden können.
Zur Eingabekontrolle wird innerhalb von Heyflow das Rollenkonzept angewendet, nach dem Rechte zur Eingabe, Änderung und Löschung von Daten entsprechend klar definierten Rollen zugewiesen sind.

Datenschutzrelevante Zusatzfunktionen des Heyflow Baukastens
Heyflow bietet die Möglichkeit, sensible Fragen als solche zu kennzeichnen („sensitive tag“). Fragen, die mit diesem Merkmal versehen sind, werden ausschließlich zur Weiterleitung an den Kunden verarbeitet und nicht im Heyflow-System gespeichert. Heyflow empfiehlt grundsätzlich allen Kunden, diese Funktion bei der Verarbeitung personenbezogener Daten zu nutzen.

Ein weiteres Feature zur Unterstützung der Datenschutzkonformität ist die automatische Löschung veralteter Endnutzerantworten. Diese Funktion kann vom Kunden in den Flow-Einstellungen aktiviert werden.

Beim Einsatz der Wiederherstellungsfunktion („Restore Function“), mit der Benutzereingaben über mehrere Besuche hinweg erhalten bleiben, wird ein zusätzliches Feld im localStorage des Endnutzer-Browsers angelegt, in dem diese Eingaben lokal gespeichert werden. Ebenso wird bei der Nutzung des Cookie-Consent-Managers von Heyflow ein Eintrag im localStorage erstellt, um die Datenschutzeinstellungen des Endnutzers für Folgebesuche zu speichern.

Wenn der Kunde die A/B-Test-Funktionalität von Heyflow nutzt, wird ein Cookie auf dem Endgerät des Endnutzers gesetzt, um sicherzustellen, dass der Endnutzer beim erneuten Besuch die gleiche Version des Flows angezeigt bekommt. Personenbezogene Daten (PII) werden für diese Zuordnung nicht verwendet.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Heyflow hat das Hosting seiner Produktangebote an führende Anbieter von Cloud-Infrastruktur ausgelagert. Die oben genannten Dienstleister unterziehen sich regelmäßig strengen Sicherheitsprüfungen und sind unter anderem nach ISO 27001, ISO 27002, ISO 27017, ISO 27018 sowie SOC 2/3 zertifiziert. Die Verfügbarkeit der Systeme wird zusätzlich durch einen dokumentierten Deployment-Prozess sichergestellt, der Pre-Release-Checklisten, Rollback-Strategien sowie kontinuierliches Monitoring umfasst.

Zur Gewährleistung von hoher Leistung und globaler Verfügbarkeit der Flows für Endnutzer setzt Heyflow ein Content Delivery Network (CDN) ein. Dieses CDN liefert statische Ressourcen – wie Bilder, Skripte und Stylesheets – über ein verteiltes Netzwerk internationaler Edge-Server aus, wobei die Bereitstellung aus geographisch nächstgelegenen Standorten erfolgt. Strategisch platzierte Serverstandorte weltweit verbessern zudem die Ladegeschwindigkeit und Reaktionszeit der Flows.

Diese CDN-Edge-Standorte und leistungsoptimierten Server werden ausschließlich zur Performance-Beschleunigung eingesetzt und verarbeiten keine Endnutzerdaten, die über Formulare übermittelt werden. Die Systeme sind vollständig von den Speichersystemen getrennt und dienen ausschließlich der Frontend-Optimierung.

Jegliche Verarbeitung personenbezogener Daten, die durch Routing- oder Caching-Prozesse der CDN-Anbieter oder globalen Performance-Knoten erfolgt, geschieht vollumfänglich im Einklang mit den geltenden Datenschutzgesetzen, insbesondere der DSGVO.

Sofern eine Datenweiterleitung außerhalb der Europäischen Union erfolgt, stellt Heyflow sicher, dass angemessene rechtliche Garantien, insbesondere durch den Abschluss von Standardvertragsklauseln (SCCs), implementiert sind.

Für die Übermittlung personenbezogener Daten aus dem Vereinigten Königreich in Drittländer gelten zusätzlich die Standardvertragsklauseln (Auftragsverarbeiter) in Verbindung mit dem vom britischen Information Commissioner’s Office (ICO) herausgegebenen UK International Data Transfer Addendum.

Weitere Informationen zu Subunternehmern sowie zu Datenübermittlungen in Drittländer finden sich in Anhang 3.

Alle über Flows auf der Heyflow-Plattform erhobenen und übermittelten Endnutzerdaten werden vorrangig innerhalb Europas gespeichert und verarbeitet. Die zentralen Datenverarbeitungsprozesse des Unternehmens sind in dieser Region angesiedelt, um eine dauerhafte Einhaltung der europäischen Datenschutzstandards sicherzustellen.

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

Die Mitarbeitenden von Heyflow werden regelmäßig für den Datenschutz sensibilisiert und zur Vertraulichkeit verpflichtet. Eine Datenschutz-Folgenabschätzung (DSFA) wird anlassbezogen und in enger Abstimmung mit den zuständigen Stellen durchgeführt.

Heyflow-Nutzer:innen sowie Endnutzer:innen finden den formellen Ablauf für Auskunftsersuchen in der geltenden Datenschutzerklärung. Sämtliche Verfahren und Richtlinien zum Datenschutz werden unternehmensweit bereitgestellt und stehen autorisierten Mitarbeitenden jederzeit zur Verfügung.

Die Wirksamkeit der technischen Schutzmaßnahmen wird halbjährlich unter Aufsicht des CTO überprüft. Zugriffsrechte, insbesondere privilegierte Zugriffe, werden mindestens einmal jährlich kontrolliert. Änderungen der Rollen oder Tätigkeitsbereiche von Mitarbeitenden führen zu einer unmittelbaren Überprüfung und Anpassung der Zugriffsrechte. Es gilt das Prinzip der funktionalen Trennung (Segregation of Duties), um unbefugten oder unbemerkten Missbrauch zu verhindern.

Kritische Sicherheitsvorfälle und Datenschutzverletzungen werden über ein Ticketing-System dokumentiert und den jeweiligen Kunden umgehend telefonisch oder per E-Mail gemeldet. Darüber hinaus informiert Heyflow über wichtige sicherheitsrelevante Updates mittels In-App-Nachrichten und betreibt eine öffentlich zugängliche Statusseite unter: https://status.heyflow.com.

Etwaige Meldepflichten gegenüber Aufsichtsbehörden werden ordnungsgemäß eingehalten.

Heyflow folgt dem Prinzip „Privacy by Default“ und erhebt nur diejenigen personenbezogenen Daten, die für die Nutzung der Dienste erforderlich sind. Die Grundsätze von „Privacy by Design“ sind über den gesamten Software-Lebenszyklus hinweg verankert.

Unterauftragsverarbeiter (Subprozessoren) werden von Heyflow im Vorfeld sorgfältig geprüft, insbesondere im Hinblick auf die implementierten Sicherheitsmaßnahmen und deren Dokumentation. Die Auswahl erfolgt unter Beachtung datenschutzrechtlicher und sicherheitsrelevanter Kriterien. Der Abschluss einer Auftragsverarbeitungsvereinbarung (Art. 28 DSGVO) oder ggf. der EU-Standardvertragsklauseln ist verbindlich vorgeschrieben.

Mitarbeitende können vermutete oder bestätigte Sicherheitsvorfälle – auch anonym – über ein internes Feedbacksystem gemäß unserer Whistleblower-Richtlinie melden.

Anhang 3: Unterauftragsverarbeiter von Endnutzerdaten

Standard-Subunternehmer (Default Sub-Prozessoren)

Google Ireland Limited

- **Adresse:** Gordon House, Barrow Street, Dublin 4, Irland
- **Umfang, Art und Zweck der Verarbeitung:** Bereitstellung und Betrieb der Server über die Google Cloud Platform
- **Kategorien betroffener Personen:** Endnutzer
- **Kategorien personenbezogener Daten:** App-Daten, Endnutzerdaten gemäß Definition durch den Verantwortlichen
- **Dauer der Verarbeitung:** Unbestimmt
- **Ort der Verarbeitung:** EU

Cloudflare, Inc.

- **Address:** 101 Townsend Street, San Francisco, CA 94107, USA
- **Umfang, Art und Zweck der Verarbeitung:**
    - Content-Delivery, Sicherheit, DNS-Verwaltung, Missbrauchsprävention
    - Verwaltung von SSL-Zertifikaten und Verbindungen für benutzerdefinierte Domains
    - Verarbeitung begrenzter personenbezogener Daten zu Protokollierungs- und Missbrauchserkennungszwecken
- **Kategorien betroffener Personen:** Endnutzer
- **Categories of Personal Data***:* IP-Addresse, User-Agent
- **Dauer der Verarbeitung:** Unbestimmt
- **Ort der Verarbeitung:** Global

Optionale / Funktionsabhängige Subunternehmer (Optional / Feature-based Sub-Prozessoren)

Amazon Web Services EMEA SARL

- **Adresse:** 38 Avenue John F. Kennedy, L-1855, Luxemburg
- **Umfang, Art und Zweck der Verarbeitung:** Versand von Anfragedaten per E-Mail an den Kunden
- **Kategorien betroffener Personen:** Endnutzer
- **Kategorien personenbezogener Daten:** Endnutzerdaten gemäß Definition durch den Kunden
- **Dauer der Verarbeitung:** Unbestimmt
- **Ort der Verarbeitung:** EU

Tinybird, Inc.

- **Adresse:** 41 East 11th Street, 11th Floor, New York, NY 10003, USA
- **Umfang, Art und Zweck der Verarbeitung:** Echtzeit-Datenverarbeitung zur Verbesserung von Abfragen und Visualisierungen innerhalb des Flow-Analytics-Dashboards
- **Kategorien betroffener Personen:** Endnutzer

- **Kategorien personenbezogener Daten:** IP-Adresse
- **Dauer der Verarbeitung:** Unbestimmt
- **Ort der Verarbeitung:** EU

tyntec Ltd.

- **Adresse:** 13th floor, One Angel Court, London EC2R 7HJ, Vereinigtes Königreich
- **Umfang, Art und Zweck der Verarbeitung:** Telefonnummernverifizierung (optionale Funktion)
- **Kategorien betroffener Personen:** Endnutzer
- **Kategorien personenbezogener Daten:** Telefonnummer (nicht direkt zuordenbar zu weiteren personenbezogenen Daten)
- **Dauer der Verarbeitung:** Unbestimmt
- **Ort der Verarbeitung:** EU / UK

Trestle Solutions, Inc.

- **Adresse:** 12819 SE 38th St #263, Bellevue, WA 98006, USA
- **Umfang, Art und Zweck der Verarbeitung:** Telefonnummernverifizierung (optionale Funktion)
- **Kategorien betroffener Personen:** Endnutzer
- **Kategorien personenbezogener Daten:** Telefonnummer (nicht direkt zuordenbar zu weiteren personenbezogenen Daten)
- **Dauer der Verarbeitung:** Unbestimmt
- **Ort der Verarbeitung:** USA, unter Einbeziehung von Standardvertragsklauseln (SCCs), Transfer Impact Assessment durchgeführt

Sinch Sweden AB

- **Adresse:** Lindhagensgatan 112, 112 51 Stockholm, Schweden
- **Umfang, Art und Zweck der Verarbeitung:** Versand von Einmalpasswörtern (OTP) per SMS zur Verifizierung (optionale Funktion)
- **Kategorien betroffener Personen:** Endnutzer
- **Kategorien personenbezogener Daten:** Telefonnummer (nicht direkt zuordenbar zu weiteren personenbezogenen Daten)
- **Dauer der Verarbeitung:** Unbestimmt
- **Ort der Verarbeitung:** EU