Bestimmungen zur Auftragsverarbeitung

Status: August 2026

Präambel

Die Parteien haben einen Vertrag geschlossen, nach dem Heyflow dem Kunden Dienstleistungen bereitstellt. Diese Bestimmungen zur Auftragsverarbeitung regeln die Verarbeitung personenbezogener Daten durch Heyflow im Zusammenhang mit diesen Dienstleistungen.

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 diesen Bestimmungen zur Auftragsverarbeitung umfassen, soweit zutreffend, auch die britische DSGVO (wie in den „Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019" definiert) 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 Art. 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 „Funnel" bezeichnet ein web-basiertes, interaktives Formular zur Erfassung von Präferenzen oder Interessen an bestimmten Produkten und Dienstleistungen.

1.2.2 „Kunde" bezeichnet jede natürliche oder juristische Person, die die Services von Heyflow nutzt und in Bezug auf die im Rahmen dieser Bestimmungen zur Auftragsverarbeitung verarbeiteten personenbezogenen Daten als Verantwortlicher (Art. 4 Nr. 7 DSGVO) handelt.

1.2.3 „Endnutzer" bezeichnet die natürliche Person, die mit einem von einem Kunden bereitgestellten Funnel interagiert oder diesen nutzt, im Rahmen der Kommunikation oder der Dienstleistungen dieses Kunden.

1.2.4 „Besuch" bezeichnet jeden Zugriff eines Endnutzers auf einen Funnel.

1.2.5 „Antwort" bezeichnet Informationen, die von einem Endnutzer bereitgestellt und aktiv über einen Funnel übermittelt werden. Jede Übermittlung gilt als eine Antwort.

1.2.6 „Partial Submits" bezeichnet eine optionale Funktionalität, die, wenn sie für einen Funnel aktiviert ist, dazu führt, dass mehrere Übermittlungen desselben Endnutzers

innerhalb einer einzelnen Funnel-Sitzung zu einer einzigen Antwort zusammengefasst und gezählt werden, anstatt separat gezählt zu werden.

1.2.7 „Response Handler" bezeichnet eine optionale Integration, die von einem Kunden konfiguriert und aktiviert werden kann und die, wenn aktiv, Antworten an das konfigurierte Zielsystem weiterleitet.

1.2.8 „Sensitive Tag" bezeichnet eine auswählbare Einstellung innerhalb der Heyflow-Anwendung, die im aktivierten Zustand darauf ausgelegt ist, die betreffenden Antworten zur Weiterleitung an den Response Handler zu leiten, anstatt sie innerhalb der Systeme von Heyflow zu speichern, vorbehaltlich der in Anhang 2 beschriebenen Ausnahmen.

1.2.9 „First-in-First-out (FIFO)" bezeichnet ein Verfahren, nach dem zusätzliche oder gespeicherte Antworten in der Reihenfolge ihres ursprünglichen Eingangs verarbeitet oder weitergeleitet werden.

1.2.10 „Consumption-Based Pricing" bezeichnet ein Abrechnungsmodell, nach dem die Nutzung einer volumenbasierten Ressource (Antworten, Besuche/Traffic oder Heyflow Credits), soweit sie das im Plan des Kunden oder in zusätzlich erworbenen Paketen enthaltene Volumen innerhalb eines bestimmten Vertragszeitraums übersteigt, automatisch und zum jeweils geltenden Preis pro Einheit gemäß den Allgemeinen Geschäftsbedingungen von Heyflow abgerechnet wird, sofern der Kunde keine zusätzlichen Pakete erwirbt.

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

1.2.12 „EWR" ist der Europäische Wirtschaftsraum.

1.2.13 „Drittland" ist jedes Land außerhalb des EWR.

1.2.14 „Leistungsvertrag" bezeichnet die entgeltliche vertragliche Vereinbarung zwischen Heyflow und einem Kunden über die Nutzung der Services von Heyflow, unabhängig davon, ob diese unmittelbar oder im Anschluss an eine Testphase geschlossen wird.

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

1.2.16 „Parteien" (oder einzeln eine „Partei") sind der Kunde und Heyflow.

1.2.17 „Services" bezeichnet die von Heyflow im Rahmen des Leistungsvertrags für den Kunden zu erbringenden Leistungen, wie in den Allgemeinen Geschäftsbedingungen von Heyflow beschrieben.

1.2.18 „Sichere Drittländer" sind alle Drittländer, für die ein Angemessenheitsbeschluss der Europäischen Kommission gemäß Art. 45 Abs. 3 DSGVO gilt.

1.2.19 „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 und/oder Modul 3, je nach Anwendbarkeit auf die jeweilige Übermittlung).

1.2.20 „Unterauftragsverarbeiter" ist jeder weitere Auftragsverarbeiter, den ein Auftragsverarbeiter gemäß Art. 28 Abs. 2 und 4 DSGVO in Anspruch nimmt.

1.2.21 „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.

1.2.22 „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.

1.2.23 „Programmatic Interface" bezeichnet jede Schnittstelle mit Ausnahme der Standard-Weboberfläche der Heyflow-Anwendung, über die ein Kunde oder ein auf Anweisung des Kunden handelndes Tool auf das Heyflow-Konto des Kunden zugreifen, dieses konfigurieren oder verwalten kann, einschließlich einer Programmierschnittstelle (Application Programming Interface, API), einer Kommandozeilenschnittstelle (Command Line Interface, CLI) und einer MCP Integration.

1.2.24 „MCP Integration" bezeichnet eine Programmatic Interface, die über das Model Context Protocol (MCP) oder ein funktional gleichwertiges Protokoll eingerichtet wird und über die ein vom Kunden im Rahmen seiner eigenen Vereinbarung mit dem jeweiligen Anbieter betriebener AI-Assistent eines Drittanbieters (z. B. Claude oder ChatGPT) auf das Heyflow-Konto des Kunden zugreifen kann, um auf Anweisung des Kunden Funnels anzuzeigen, zu erstellen, zu bearbeiten, zu veröffentlichen oder anderweitig zu verwalten.

1.2.25 „AI Output" bezeichnet Inhalt, Design, Struktur, Ablauflogik, Weiterleitungen und sonstige Konfiguration eines Funnels, die mithilfe des eigenen AI-Assistenten von Heyflow oder eines über eine MCP Integration oder eine andere Programmatic Interface zugänglichen AI-Assistenten eines Drittanbieters erzeugt, vorgeschlagen oder verändert werden.

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 Funnels zur Verfügung. Grundsätzlich obliegt die Ausgestaltung der Funnels durch die Verwendung des Baukastens dem Kunden. Heyflow kann die Art der durch einen Funnel erhobenen Daten nicht pauschal eingrenzen. Heyflow stellt dem Kunden jedoch eine optionale Funktion zur Verfügung – die in Anhang 2 beschriebene Sensitive-Tag-Funktionalität –, die darauf ausgelegt ist, die Speicherung personenbezogener Daten von Endnutzern zu begrenzen, vorbehaltlich der dort beschriebenen Ausnahmen. Die sachgemäße Verwendung dieser Funktion obliegt dem Kunden.

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

2.4 Verarbeitet der Kunde im Rahmen der Nutzung der Services geschützte Gesundheitsinformationen („Protected Health Information", „PHI") im Sinne des US-amerikanischen Health Insurance Portability and Accountability Act („HIPAA"), gilt für eine solche Verarbeitung eine gesonderte, zwischen dem Kunden und Heyflow abgeschlossene Vereinbarung („Business Associate Agreement", „BAA"). Im Falle eines Widerspruchs zwischen diesen Bestimmungen zur Auftragsverarbeitung und dem BAA hinsichtlich der Verarbeitung von PHI hat das BAA Vorrang.

2.5 In Bezug auf personenbezogene Daten von Einwohnern Kaliforniens, die im Rahmen dieser Bestimmungen zur Auftragsverarbeitung verarbeitet werden, handelt Heyflow als „Dienstleister" („Service Provider") im Sinne des CCPA. Heyflow verkauft oder gibt solche personenbezogenen Daten nicht weiter und verarbeitet sie ausschließlich zu den vom Kunden festgelegten Geschäftszwecken („Business Purposes") und zu keinem anderen Zweck.

2.6 Sofern in Ziffer 5.4 (Beauftragung weiterer Auftragsverarbeiter) und Ziffer 6 (Übermittlung personenbezogener Daten an Drittländer) nicht etwas anderes bestimmt ist, unterliegen Änderungen dieser Bestimmungen zur Auftragsverarbeitung dem in den Allgemeinen Geschäftsbedingungen von Heyflow festgelegten Änderungs- und Widerspruchsverfahren.

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 und Pflichten des Kunden

4.1 Weisungsrecht

4.1.1 Der Verantwortliche behält sich das Recht vor, den Auftragsverarbeiter hinsichtlich der Verarbeitung personenbezogener Daten nach diesen Bestimmungen zur Auftragsverarbeitung anzuweisen.

4.1.2 Die Bestimmungen dieser Bestimmungen zur Auftragsverarbeitung, insbesondere die in Ziffer 3 dargelegten Einzelheiten der Verarbeitung, stellen allgemeine Weisungen zur Verarbeitung personenbezogener Daten dar, soweit dies für die Erbringung der Services erforderlich ist, im Einklang mit diesen Bestimmungen zur Auftragsverarbeitung und dem Leistungsvertrag.

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 Art. 28 DSGVO niedergelegten Pflichten zu verlangen und, entweder unmittelbar oder durch einen vom Verantwortlichen beauftragten Prüfer, Überprüfungen – einschließlich Inspektionen – in den Räumlichkeiten des Auftragsverarbeiters durchzuführen.

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 der gut begründeten Auffassung, dass diese zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten nicht ausreichend sind, oder dass Heyflow seine Pflichten aus Art. 28 DSGVO oder diesen Bestimmungen zur Auftragsverarbeitung verletzt hat, hat der Kunde das Recht, Überprüfungen – einschließlich Inspektionen – bei Heyflow entweder selbst oder durch einen von ihm beauftragten Prüfer durchzuführen.

4.2.4 Der Kunde hat Heyflow mindestens zwei (2) Wochen im Voraus über die Durchführung einer Überprüfung, einschließlich einer Inspektion, zu informieren.

4.2.5 Heyflow darf Inspektionen außerhalb der normalen Geschäftszeiten 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 Grundes.

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, anzufertigen, 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 Heyflow nicht durch das Recht der Union, der Mitgliedstaaten oder des Vereinigten Königreichs, 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 Recht der Union, der Mitgliedstaaten oder des Vereinigten Königreichs zur Verarbeitung verpflichtet ist.

5.1.3 Heyflow informiert den Kunden unverzüglich, wenn Heyflow der Auffassung ist, dass eine vom Kunden erteilte Weisung gegen die DSGVO, die britische DSGVO oder andere anwendbare Datenschutzbestimmungen der Union, ihrer Mitgliedstaaten oder des Vereinigten Königreichs verstößt. Heyflow ist berechtigt, die Ausführung der jeweiligen Weisung auszusetzen, bis diese vom Kunden bestätigt oder geändert wurde.

5.1.4 Heyflow verwendet Antworten (personenbezogene Daten, die von Endnutzern über einen Funnel übermittelt werden) nicht zum Training, zur Feinabstimmung, zur Bewertung oder auf sonstige Weise zur Entwicklung oder Verbesserung eines von Heyflow oder einem Dritten betriebenen AI- oder Machine-Learning-Modells.

5.2 Vertraulichkeit der zur Verarbeitung personenbezogener Daten berechtigten Personen

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

5.3 Sicherheit der Verarbeitung

5.3.1 Heyflow ergreift alle gemäß Art. 32 DSGVO erforderlichen Maßnahmen.

5.3.2 Die konkreten 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 Wird Heyflow eine Verletzung des Schutzes personenbezogener Daten, die Gegenstand dieser Bestimmungen zur Auftragsverarbeitung sind, bekannt, meldet Heyflow diese dem Kunden unverzüglich.

5.3.5 Der Kunde trägt die Kosten, die ihm für die Erfüllung seiner Verpflichtungen aus einer Verletzung des Schutzes personenbezogener Daten entstehen, sowie etwaige angemessene Unterstützungskosten Heyflows, es sei denn, die Verletzung beruht auf einem schuldhaften Verstoß des Auftragsverarbeiters gegen diese Bestimmungen zur Auftragsverarbeitung oder gegen dokumentierte Weisungen des Verantwortlichen.

5.4 Beauftragung weiterer Auftragsverarbeiter

5.4.1 Heyflow hält die folgenden in Art. 28 Abs. 2 und 4 DSGVO genannten Bedingungen für die Beauftragung eines weiteren Auftragsverarbeiters ein:

a) Heyflow informiert den Kunden unverzüglich über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung weiterer Unterauftragsverarbeiter und ermöglicht dem Kunden dadurch, hiergegen erforderlichenfalls Einspruch zu erheben.

b) Nimmt Heyflow die Dienste eines weiteren Unterauftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten für den Kunden auszuführen, so werden diesem Unterauftragsverarbeiter im Wege eines Vertrags oder eines anderen Rechtsinstruments im Sinne von Art. 28 DSGVO dieselben Datenschutzpflichten auferlegt, wie sie in diesen Bestimmungen zur Auftragsverarbeitung festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass

geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung den Anforderungen der DSGVO entspricht.

c) Kommt der weitere Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, haftet Heyflow gegenüber dem Kunden für die Einhaltung der Pflichten jenes weiteren Unterauftragsverarbeiters.

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

5.4.3 Weist der Kunde Heyflow nach, dass eine beabsichtigte Änderung hinsichtlich der Hinzuziehung oder Ersetzung von Unterauftragsverarbeitern für ihn – unter Berücksichtigung aller Umstände und unter Abwägung der Interessen beider Seiten – nicht zumutbar ist, und legt er 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 Genehmigung des Kunden beauftragten weiteren Auftragsverarbeiter fortzuführen, oder

b) alle Maßnahmen zu ergreifen, um den vom Kunden geltend gemachten Widerspruchsgrund zu beseitigen, den Kunden hierüber zu informieren und ihm erneut ein entsprechendes Widerspruchsrecht einzuräumen, und 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 innerhalb von 14 Tagen nach Ablauf der Widerspruchsfrist die Möglichkeit einer Sonderkündigung des Vertragsverhältnisses mit sofortiger Wirkung eingeräumt.

Dieses Verfahren gilt auch für eine sich daraus ergebende Übermittlung der Verarbeitung in ein Drittland (siehe Ziffer 6.1).

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

5.5.1 Heyflow unterstützt den Kunden unter Berücksichtigung 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 von DSGVO-Pflichten

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

Art. 32 bis 36 DSGVO genannten Pflichten in Bezug auf personenbezogene 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 dieser Bestimmungen zur Auftragsverarbeitung sind, oder gibt diese an den Kunden zurück und löscht die vorhandenen Kopien, sofern nicht nach dem Recht der Union oder der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

5.8 **Externer Datenschutzdienstleister**

5.8.1 Heyflow nimmt die Dienste des externen Datenschutzdienstleisters PROLIANCE GmbH (www.datenschutzexperte.de), Dominik Fünkner, Leopoldstr. 21, 80802 München, in Anspruch; Fragen und Anliegen zum Datenschutz sind an datenschutzbeauftragter@datenschutzexperte.de zu richten.

6. Übermittlung personenbezogener Daten an Drittländer

6.1 Eine Übermittlung personenbezogener Daten in ein Drittland darf nur erfolgen, wenn die besonderen Voraussetzungen für eine solche Übermittlung nach Art. 44 ff. DSGVO erfüllt sind, insbesondere durch die Verwendung von Standardvertragsklauseln (Auftragsverarbeiter) oder eines anwendbaren Angemessenheitsbeschlusses gemäß Art. 45 DSGVO. Für die Übermittlung personenbezogener Daten aus dem Vereinigten Königreich in Drittländer gelten die Standardvertragsklauseln (Auftragsverarbeiter) in Verbindung mit dem vom britischen Information Commissioner's Office herausgegebenen UK International Data Transfer Addendum. Erfolgt die Übermittlung an einen von Heyflow beauftragten Unterauftragsverarbeiter (im Gegensatz zu einer Übermittlung durch den Kunden als Verantwortlichen an Heyflow als Auftragsverarbeiter), findet Modul 3 (Auftragsverarbeiter zu Auftragsverarbeiter) der Standardvertragsklauseln (Auftragsverarbeiter) Anwendung.

6.2 Ergibt sich eine Übermittlung der Verarbeitung in ein Drittland aus der Beauftragung oder Ersetzung eines Unterauftragsverarbeiters, gilt das in Ziffer 5.4 festgelegte Mitteilungs- und Widerspruchsverfahren; ein gesondertes Mitteilungs- oder Widerspruchsrecht nach dieser Ziffer 6 besteht in diesem Fall nicht. Ergibt sich eine Übermittlung der Verarbeitung in ein Drittland aus einem anderen Grund als der Beauftragung oder Ersetzung eines Unterauftragsverarbeiters, informiert Heyflow den Kunden vorab in Textform (z. B. per E-Mail); der Kunde kann der Übermittlung innerhalb von zwei (2) Wochen nach Erhalt dieser Information schriftlich oder in Textform unter Angabe einer Begründung widersprechen. Ziffer 5.4.3 lit. a) und b) gelten für einen solchen Widerspruch entsprechend.

7. Haftung

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

8. Laufzeit und Beendigung

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

Anhänge:

Anhang 1: Einzelheiten der Verarbeitung

Anhang 2: Technische und organisatorische Maßnahmen Heyflows

Anhang 3: Unterauftragsverarbeiter von 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 Funnels. Funnels sind vom Kunden individuell anpassbar, werden jedoch typischerweise verwendet, um Präferenzen von Endnutzern, Produktinteressen oder Bewerbungen zu erfassen.
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 und zum Betrieb von Funnels zur Verfügung. Kunden können ihre Funnels über technische Schnittstellen mit Diensten von Drittanbietern verknüpfen, etwa mit Werbeplattformen oder Kundenmanagementsystemen. Diese Integrationen werden innerhalb der Heyflow-Webanwendung verwaltet, und die damit zusammenhängende Datenverarbeitung erfolgt durch Heyflow auf Grundlage ausdrücklicher In-App-Anweisungen. Heyflow kann zudem intern AI-Anbieter von Drittanbietern (siehe Anhang 3) einsetzen, um den eigenen AI-Assistenten von Heyflow und andere Funktionen zur Erzeugung von AI Output zu betreiben und um allgemein zur Erbringung von Teilen des Services beizutragen, einschließlich im Zusammenhang mit Anfragen, die über die MCP Integration oder eine andere Programmatic Interface eingehen.
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 Erhebung von personenbezogenen Daten wie beispielsweise Name, Adresse, E-Mail und Telefonnummer. Die Übermittlung formularspezifischer Daten hängt davon ab, wie der Kunde den jeweiligen Funnel konfiguriert hat, einschließlich der Frage, welche Bausteine – etwa die Schaltfläche „Absenden", der Stripe-Zahlungsblock oder ein anderer konfigurierbarer Baustein – zur Auslösung der Datenübermittlung konfiguriert sind. Zusätzlich kann über die Heyflow-App eine Zustimmungsfunktion integriert werden.

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 erhoben.

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 sowie nach SOC 2 Typ II zertifiziert (unter Abdeckung der Trust Services Criteria „Security" und „Confidentiality", unabhängig geprüft) und werden regelmäßig sowohl intern als auch extern geprüft. Heyflow stellt einen aktuellen Überblick über den jeweiligen Compliance-Status, einschließlich der aktuellen Zertifizierungszeiträume und -berichte, 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 (Art. 32 Abs. 1 lit. b DSGVO)

IT-Infrastruktur
Für das Hosting seines Produktangebots setzt Heyflow auf führende, state-of-the-art Cloud-Infrastruktur. Diese Lösung verspricht einen hohen Grad an physischer Sicherheit und Netzwerksicherheit. Die von Heyflow angemieteten Server befinden sich ausschließlich in der Europäischen Union. Die Server selbst werden bei Google Cloud Platform gehostet, das regelmäßig strenge Sicherheitsaudits durchläuft und unter anderem nach ISO 27001, ISO 27002, ISO 27017, ISO 27018 und SOC 2/3 zertifiziert ist. Die physischen, umgebungsbezogenen und infrastrukturellen Sicherheitsvorkehrungen wurden im Rahmen der ISO-27001- und SOC-2-Type-2-Zertifizierungen von unabhängigen Stellen bestätigt.
Die entsprechenden Zertifikate können unter folgendem Link eingesehen werden: https://cloud.google.com/security/compliance/offerings.

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 autorisiertem Fachpersonal 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 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.

Endnutzerdaten, die zwischen Nutzern oder Kunden und den öffentlichen Produktionsendpunkten von Heyflow übertragen werden, sind bei der Übertragung mittels TLS 1.2 oder TLS 1.3 verschlüsselt. Diese Endpunkte verwenden eingeschränkte, moderne Cipher Suites; die jeweilige Cipher Suite und der Schlüsselaustauschmechanismus werden für jede Verbindung neu ausgehandelt, wobei Forward Secrecy dort bereitgestellt wird, wo dies unterstützt wird. Versendet Heyflow Endnutzerdaten per E-Mail, ist die Verbindung mittels TLS verschlüsselt. Die Zustellung von E-Mails an den empfangenden Mailserver des Kunden erfolgt über TLS, sofern der empfangende Server dies unterstützt.

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 werden – unabhängig davon, ob sie sich in Übertragung oder in Speicherung befinden – 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.

Die Übermittlung personenbezogener Daten an Heyflow oder dessen Unterauftragsverarbeiter hängt davon ab, wie der Kunde den jeweiligen Funnel konfiguriert hat. Jeder relevante Baustein – etwa die Schaltfläche „Absenden", der Stripe-Zahlungsblock oder ein anderer konfigurierbarer Baustein – steht dem Kunden innerhalb der Heyflow-Anwendung zur Verfügung und muss von diesem ausdrücklich konfiguriert und aktiviert werden. Personenbezogene Daten werden an Heyflow oder dessen Unterauftragsverarbeiter nur entsprechend dieser Konfiguration übermittelt.

Beim Zugriff auf einen Funnel und während der Navigation 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.

Heyflow bietet eine Integration („MCP Integration") an, die es dem Kunden ermöglicht, einen AI-Assistenten eines Drittanbieters (z. B. Claude oder ChatGPT), der vom Kunden im Rahmen seines eigenen Kontos und seiner eigenen Vereinbarung mit dem jeweiligen Anbieter betrieben wird, mit dem Heyflow-Konto des Kunden zu verbinden, um auf Anweisung des Kunden Funnels anzuzeigen, zu erstellen, zu bearbeiten oder zu verwalten. Daten, die im Rahmen dieser Verbindung unmittelbar zwischen dem eigenen AI-Assistenten des Kunden und dessen Anbieter ausgetauscht werden, werden im Rahmen der eigenen Vereinbarung des Kunden mit diesem Anbieter verarbeitet; Heyflow ist an dieser Verarbeitung nicht beteiligt und übernimmt hierfür keine Verantwortung.

Getrennt davon setzt Heyflow selbst AI-Anbieter von Drittanbietern ein, um den eigenen AI-Assistenten von Heyflow und andere AI-gestützte Funktionen zur Erzeugung von AI Output zu betreiben und um allgemein zur Erbringung von Teilen des Services beizutragen, einschließlich im Zusammenhang mit Anfragen, die über die MCP Integration oder eine andere Programmatic Interface eingehen. In jedem Fall nutzt Heyflow dabei sein eigenes Konto und seine eigenen Zugangsdaten bei dem jeweiligen Anbieter – der Kunde verbindet kein eigenes Konto. Der bzw. die betreffenden Anbieter werden für diesen Zweck als Unterauftragsverarbeiter von Heyflow eingesetzt und sind in Anhang 3 aufgeführt, unabhängig davon, ob die jeweilige Verarbeitung im Einzelfall personenbezogene Daten betrifft. Antworten von Endnutzern sind über die MCP Integration derzeit nicht zugänglich.

Sollte Heyflow zukünftig den Abruf von Antworten über die MCP Integration ermöglichen, steht ein solcher Abruf ausschließlich Kunden zur Verfügung, die hierfür eine gesonderte, kontobezogene Einstellung aktiviert haben, die von der Aktivierung der MCP Integration selbst unabhängig ist.

Softwareentwicklung und -veränderungen
Programmgesteuerte Änderungen an den von Heyflow bereitgestellten Diensten werden mit Hilfe 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: die Verwendung getrennter Umgebungen (Development, Staging, Production), automatisierte Regressionstests, Peer Reviews (Vier-Augen-Prinzip) sowie manuelle Qualitätssicherungsprüfungen (QA) vor der Bereitstellung in der Produktivumgebung. Die Entwickler:innen erhalten regelmäßig Schulungen zum sicheren Programmieren, insbesondere zur Vermeidung von Bedrohungen gemäß OWASP Top 10. Zur weiteren Erhöhung der Sicherheit führt Heyflow jährlich Penetrationstests durch, 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 Funktionalität „Sensitive Tag" an, die im aktivierten Zustand darauf ausgelegt ist, die betreffenden Antworten zur Weiterleitung an den vom Kunden konfigurierten Response Handler zu leiten, anstatt sie innerhalb der Systeme von Heyflow zu speichern. Ist das Antwortkontingent des Kunden überschritten und unterliegt der Kunde nicht dem Consumption-Based Pricing, so werden weitere Antworten – einschließlich solcher, die mit einem Sensitive Tag versehen sind – ungeachtet der Sensitive-Tag-Einstellung im System von Heyflow gespeichert und nach dem First-in-First-out-Prinzip (FIFO) weitergeleitet, sobald zusätzliches

Antwortkontingent erworben wurde. Unterliegt der Kunde dagegen dem Consumption-Based Pricing, so werden Antworten weiterhin entsprechend der Konfiguration – einschließlich der jeweiligen Sensitive-Tag-Einstellung – weitergeleitet und verarbeitet, unabhängig vom Kontingent. Heyflow empfiehlt grundsätzlich allen Kunden, die Sensitive-Tag-Funktionalität für personenbezogene Daten zu nutzen und, soweit sie nicht dem Consumption-Based Pricing unterliegen, ihr Antwortkontingent entsprechend zu überwachen.

Ein weiteres Feature zur Unterstützung der Datenschutzkonformität ist die automatische Löschung veralteter Endnutzerantworten. Diese Funktion kann vom Kunden in den Funnel-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 Funnels angezeigt bekommt. Personenbezogene Daten (PII) werden für diese Zuordnung nicht verwendet.

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

Das Server-Hosting von Heyflow erfolgt, wie vorstehend beschrieben, über Google Cloud Platform, die regelmäßig strenge Sicherheitsaudits durchläuft und unter anderem nach ISO 27001, ISO 27002, ISO 27017, ISO 27018 sowie SOC 2/3 zertifiziert ist. 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 Funnels 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 geografisch nächstgelegenen Standorten erfolgt. Strategisch platzierte Serverstandorte weltweit verbessern zudem die Ladegeschwindigkeit und Reaktionszeit der Funnels.

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 implementiert sind, insbesondere durch den Abschluss von Standardvertragsklauseln (SCCs).

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 Unterauftragsverarbeitern sowie zu Datenübermittlungen in Drittländer finden sich in Anhang 3.

Die vorstehend beschriebene Hosting-Infrastruktur – d. h. die Server, auf denen Endnutzerdaten gespeichert werden – befindet sich vorrangig innerhalb Europas, und die zentralen Hosting-Prozesse des Unternehmens sind in dieser Region angesiedelt, um eine dauerhafte Übereinstimmung mit den europäischen Datenschutzstandards sicherzustellen. Diese Aussage bezieht sich ausschließlich auf das Server-Hosting; die vollständige Liste der an der Verarbeitung von Endnutzerdaten beteiligten Unterauftragsverarbeiter, einschließlich solcher außerhalb der EU/des EWR, ist in Anhang 3 aufgeführt.

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 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 gegebenenfalls 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-Unterauftragsverarbeiter

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.

- **Adresse:** 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
- **Kategorien personenbezogener Daten:** IP-Adresse, User-Agent
- **Dauer der Verarbeitung:** Unbestimmt
- **Ort der Verarbeitung:** Global

Anthropic PBC

- **Adresse:** 548 Market Street, PMB 90375, San Francisco, CA 94104, USA
- **Umfang, Art und Zweck der Verarbeitung:** Interne Nutzung von AI-Modellen durch Heyflow, um den eigenen AI-Assistenten von Heyflow und andere AI-gestützte Funktionen zur Erzeugung von AI Output zu betreiben (z. B. Interpretation von Anweisungen, Erzeugung oder Strukturierung von Funnel-Inhalten) und um allgemein zur Erbringung von Teilen des Services beizutragen, einschließlich – jedoch nicht beschränkt auf – Anfragen, die über die MCP Integration eingehen. Dieser Eintrag gilt unabhängig davon, ob die jeweilige Verarbeitung im Einzelfall personenbezogene Daten betrifft.
- **Kategorien betroffener Personen:** Endnutzer und/oder Nutzer des Kunden, soweit personenbezogene Daten zufällig in den verarbeiteten Inhalten enthalten sind.
- **Kategorien personenbezogener Daten:** Variiert je nach Funktion; überwiegend Funnel-Struktur-/Konfigurationsdaten, die zufällig personenbezogene Daten enthalten können (z. B. Platzhaltertext, Testübermittlungen oder Kontometadaten)
- **Dauer der Verarbeitung:** Unbestimmt
- **Ort der Verarbeitung:** USA, Standardvertragsklauseln finden Anwendung, Transfer Impact Assessment durchgeführt

OpenAI Ireland Limited

- **Adresse:** 1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43, Irland
- **Umfang, Art und Zweck der Verarbeitung:** Interne Nutzung von AI-Modellen durch Heyflow, um den eigenen AI-Assistenten von Heyflow und andere AI-gestützte Funktionen zur Erzeugung von AI Output zu betreiben (z. B. Interpretation von Anweisungen,

Erzeugung oder Strukturierung von Funnel-Inhalten) und um allgemein zur Erbringung von Teilen des Services beizutragen, einschließlich – jedoch nicht beschränkt auf – Anfragen, die über die MCP Integration eingehen. Dieser Eintrag gilt unabhängig davon, ob die jeweilige Verarbeitung im Einzelfall personenbezogene Daten betrifft.
- **Kategorien betroffener Personen:** Endnutzer und/oder Nutzer des Kunden, soweit personenbezogene Daten zufällig in den verarbeiteten Inhalten enthalten sind.
- **Kategorien personenbezogener Daten:** Variiert je nach Funktion; überwiegend Funnel-Struktur-/Konfigurationsdaten, die zufällig personenbezogene Daten enthalten können (z. B. Platzhaltertext, Testübermittlungen oder Kontometadaten)
- **Dauer der Verarbeitung:** Unbestimmt
- **Ort der Verarbeitung:** EU

Optionale / funktionsabhängige Unterauftragsverarbeiter

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 von Funnel-Analysen; Unterstützung der Analytics-Dashboard-Funktionalität
- **Kategorien betroffener Personen:** Endnutzer
- **Kategorien personenbezogener Daten:** IP-Adresse
- **Dauer der Verarbeitung:** Unbestimmt
- **Ort der Verarbeitung:** EU

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, 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