

## Auftragsverarbeitungsvertrag i. S. d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO).

### Präambel

Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten.

### 1. Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Aus dem Vertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung. Im Einzelnen sind insbesondere die folgenden Daten Bestandteil der Datenverarbeitung:

Art der Daten	Art und Zweck der Datenverarbeitung	Kategorien betroffener Personen
Daten der Kunden des Auftraggebers (insb. Name, Adressdaten, Präferenzdaten)	Auftragserfüllung	Kunden des Auftraggebers
Kontaktinformation der Mitarbeiter des Auftraggebers	Auftragserfüllung	Mitarbeiter des Auftraggebers
Rechnungsadresse des Auftraggebers (inkl. Kontakt)	Auftragsabrechnung	Mitarbeiter des Auftraggebers

Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser Anlage nicht darüber hinausgehende Verpflichtungen ergeben.

### 2. Anwendungsbereich und Verantwortlichkeit

- 2.1. Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DS-GVO).
- 2.2. Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

### 3. Pflichten des Auftragnehmers

- 3.1. Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.
- 3.2. Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die

den Anforderungen der Datenschutz- Grundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

Diese technischen und organisatorischen Maßnahmen sind in der beigefügten **Anlage „Technische und organisatorische Maßnahmen“** aufgelistet. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

- 3.3. Der Auftragnehmer unterstützt - soweit vereinbart - den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten.
- 3.4. Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.
- 3.5. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden.  
Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.
- 3.6. Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.
- 3.7. Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.
- 3.8. Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart.  
In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe. Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart.
- 3.9. Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen.  
Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

3.10. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

#### **4. Pflichten des Auftraggebers**

- 4.1. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
- 4.2. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt §3 Abs. 10 entsprechend.
- 4.3. Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

#### **5. Anfragen betroffener Personen**

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

#### **6. Nachweismöglichkeiten**

- 6.1. Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.
- 6.2. Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.  
Der Auftraggeber stimmt der Benennung eines unabhängigen externen Prüfers durch den Auftragnehmer zu, sofern der Auftragnehmer eine Kopie des Auditberichts zur Verfügung stellt.  
Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.
- 6.3. Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer beruflichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

#### **7. Subunternehmer (weitere Auftragsverarbeiter)**

- 7.1. Der Auftragsverarbeiter wird den Auftragnehmer vor jeder beabsichtigten Änderung in Bezug auf die Hinzuziehung oder die Ersetzung eines Subunternehmens informieren. Der Auftragnehmer kann gegen

eine beabsichtigte Hinzuziehung oder die Ersetzung eines Subunternehmens aus wichtigem datenschutzrechtlichen Grund Einspruch erheben. Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.

Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung folgender Subunternehmer durchgeführt:

Name und Anschrift des Subunternehmers	Beschreibung der Teilleistungen
<b>DATEN_PARTNER</b> <b>Gesellschaft für Direktmarketing und Informations-Technologie mbH</b>  Feldheider Str. 39 – 45 40699 Erkrath  Deutschland (EU)	Druck- und Versand der personalisierten Werbemittel
<b>STRATO AG</b>  Pascalstraße 10 10587 Berlin  Deutschland (EU)	Die kundenindividuellen Werbemittel (inkl. der oben genannten Kundendaten des Auftraggebers) werden in Rechenzentren der STRATO AG berechnet.
<b>QualityHosting AG</b>  Uferweg 40-42 63571 Gelnhausen  Deutschland (EU)  <b>Microsoft Ireland Operations Limited</b>  Leopardstown, Dublin 18, D18 P521, Irland (EU)	Nutzung von Microsoft Office 365: <ul style="list-style-type: none"> <li>• Exchange (Kommunikation mit dem Auftraggeber)</li> <li>• Teams (Telefonkonferenzen, Webtelefonie)</li> <li>• SharePoint, OneDrive (Dateiablage und -versionierung)</li> </ul>
<b>SoftwareONE Deutschland GmbH</b>  Blochstraße 1 04329 Leipzig  Deutschland (EU)	Nutzung von Azure über SoftwareONE als End-to-End Software und Cloud-Technologielösung Anbieter.
<b>HubSpot, Inc.</b>  25 1st Street  Cambridge  MA 0214  USA	Speicherung der Rechnungsadresse des Auftraggebers zur Rechnungstellung

Vor der Hinzuziehung weiterer oder der Ersetzung aufgeführter Subunternehmer holt der Auftragnehmer die Zustimmung des Auftraggebers ein, wobei diese nicht ohne wichtigen datenschutzrechtlichen Grund verweigert werden darf.

7.2. Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.

## 8. Informationspflichten, Schriftformklausel, Rechtswahl

8.1. Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher« im Sinne der Datenschutz-Grundverordnung liegen.

8.2. Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

8.3. Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

8.4. Es gilt deutsches Recht.

## 9. Haftung und Schadensersatz

Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

## 10. Kosten und Auslagen

10.1. Soweit datenschutzrechtliche Verpflichtung, die dem Auftraggeber obliegen, auf Weisung des Auftraggebers vom Auftragnehmer erfüllt werden, hat der Auftraggeber diese Leistungen zu vergüten.

10.2. Kosten und Auslagen für Kontrollen bzw. Inspektionen durch den Auftraggeber, insbesondere Kosten für nicht Anlass bezogene Kontrollen, kann der Auftragnehmer zudem vom Auftraggeber ersetzt verlangen. Von der vorstehenden Regelung in Satz 1 ausgenommen sind Kontrollen, die der Auftraggeber im Rahmen der Erfüllung seiner gesetzlichen Kontrollpflichten durchführt.

10.3. Die Höhe der Vergütung und die Abrechnungsmodalitäten ergeben sich aus der mit dem Angebot versandten Preisliste.

## TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

### 1. Einleitung

#### 1.1. Verantwortlicher

Verantwortlicher gem. Art. 4 Abs. 7 EU-Datenschutz-Grundverordnung (DSGVO) ist AutLay - Automatisches Layout GmbH, Unter Käster 14-16, 50667 Köln, Deutschland, E-Mail: mail@autlay.com. Gesetzlich vertreten werden wir durch Dr. David Schölgens, Sven Müller.

#### 1.2. Datenschutzbeauftragter

Unser Datenschutzbeauftragter ist die heyData GmbH, Gormannstr. 14, 10119 Berlin, www.heydata.eu, E-Mail: info@heydata.de.

#### 1.3. Gegenstand des Dokuments

Dieses Dokument fasst die vom Verantwortlichen getroffenen technische und organisatorische Maßnahmen im Sinne von Art. 32 Abs. 1 DSGVO zusammen. Das sind Maßnahmen, mit denen der Verantwortliche personenbezogene Daten schützt. Das Dokument hat den Zweck, den Verantwortlichen bei der Erfüllung seiner Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO zu unterstützen.

### 2. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

#### 2.1. Zutrittskontrolle

Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zutritt zu den Datenverarbeitungsanlagen haben:

- Manuelles Schließsystem (z.B. Schlüssel)
- Sicherheitsschlösser
- Schlüsselregelung / Schlüsselbuch
- Sorgfältige Auswahl des Reinigungspersonals

#### 2.2. Zugangskontrolle

Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zugang zu den Datenverarbeitungssystemen haben:

- Authentifikation mit Benutzer und Passwort
- Authentifikation mit biometrischen Daten
- Einsatz von Mobile Device Management
- Verschlüsselung von Datenträgern
- Verschlüsselung von Notebooks / Tablets
- Verwaltung von Benutzerberechtigungen
- Erstellen von Benutzerprofilen
- Zentrale Passwortregeln
- Nutzung von 2-Faktor-Authentifizierung
- Schlüsselregelung / Schlüsselbuch

### 2.3. Zugriffskontrolle

Folgende implementierte Maßnahmen stellen sicher, dass Unbefugte keinen Zugriff auf personenbezogene Daten haben:

- Einsatz von Aktenvernichtern (mit cross cut-Funktion)
- Protokollierung von Zugriffen auf Anwendungen (insbesondere bei der Eingabe, Änderung und Löschung von Daten)
- Einsatz eines Berechtigungskonzepts
- Anzahl der Administratoren ist so klein wie möglich gehalten
- Verwaltung der Benutzerrechte durch Systemadministratoren

### 2.4. Trennungskontrolle

Folgende Maßnahmen stellen sicher, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden:

- Trennung von Produktiv- und Testsystem
- Logische Mandantentrennung (softwareseitig)
- Erstellung eines Berechtigungskonzepts
- Festlegung von Datenbankrechten

## 3. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

### 3.1. Weitergabekontrolle

Es ist sichergestellt, dass personenbezogene Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und überprüft werden kann, welche Personen oder Stellen personenbezogene Daten erhalten haben. Zur Sicherstellung sind folgende Maßnahmen implementiert:

- WLAN-Verschlüsselung (WPA2 mit starkem Passwort)

### 3.2. Eingabekontrolle

Durch folgende Maßnahmen ist sichergestellt, dass geprüft werden kann, wer personenbezogene Daten zu welcher Zeit in Datenverarbeitungsanlagen verarbeitet hat:

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Nachvollziehbarkeit der Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

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

Durch folgende Maßnahmen ist sichergestellt, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt und für den Auftraggeber stets verfügbar sind:

- Hosting (jedenfalls der wichtigsten Daten) mit einem professionellen Hoster

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

### 5.1. Datenschutz-Management

Folgende Maßnahmen sollen gewährleisten, dass eine den datenschutzrechtlichen Grundanforderungen genügende Organisation vorhanden ist:

- Verwendung der heyData-Plattform zum Datenschutz-Management
- Bestellung des Datenschutzbeauftragten heyData
- Verpflichtung der Mitarbeiter auf das Datengeheimnis
- Regelmäßige Schulungen der Mitarbeiter im Datenschutz
- Führen einer Übersicht über Verarbeitungstätigkeiten (Art. 30 DSGVO)
- Durchführung von Datenschutzfolgenabschätzungen, soweit erforderlich (Art. 35 DSGVO)

### 5.2. Incident-Response-Management

Folgende Maßnahmen sollen gewährleisten, dass im Fall von Datenschutzverstößen Meldeprozesse ausgelöst werden:

- Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Aufsichtsbehörden (Art. 33 DSGVO)
- Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Betroffenen (Art. 34 DSGVO)
- Einbindung des Datenschutzbeauftragten in Sicherheitsvorfälle und Datenpannen

### 5.3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Die folgenden implementierten Maßnahmen tragen den Voraussetzungen der Prinzipien "Privacy by design" und "Privacy by default" Rechnung:

- Schulung der Mitarbeiter im "Privacy by design" und "Privacy by default"
- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.

### 5.4. Auftragskontrolle

Durch folgende Maßnahmen ist sichergestellt, dass, dass personenbezogene Daten nur entsprechend der Weisungen verarbeitet werden können:

- Schriftliche Weisungen an den Auftragnehmer oder Weisungen in Textform (z.B. durch Auftragsverarbeitungsvertrag)
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags, z.B. durch Anfrage entsprechender Bestätigungen
- Bestätigung von Auftragnehmern, dass sie ihre eigenen Mitarbeiter auf das Datengeheimnis verpflichten (typischerweise im Auftragsverarbeitungsvertrag)
- Sorgfältige Auswahl von Auftragnehmern (insbesondere hinsichtlich Datensicherheit)