Auftragsverarbeitungsvertrag

zwischen

als Verantwortlicher (nachfolgend „**Verantwortlicher**“),

und

ContractHero GmbH, Reichardtstrasse 3, 06114 Halle (Saale), Deutschland

als Auftragsverarbeiter (nachfolgend „**Auftragsverarbeiter**“,

Verantwortlicher und Auftragsverarbeiter gemeinsam die “**Parteien**”)

Präambel

Der Verantwortliche hat den Auftragsverarbeiter im bereits geschlossenen Vertrag (nachfolgend „**Hauptvertrag**“) zu den dort genannten Leistungen beauftragt. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art. 28 DSGVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien den nachfolgenden Auftragsverarbeitungsvertrag (nachfolgend die “**Vereinbarung**”), dessen Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

§ 1 Begriffsbestimmungen

(1) Verantwortlicher ist gem. Art. 4 Abs. 7 DSGVO die Stelle, die allein oder gemeinsam mit anderen Verantwortlichen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

(2) Auftragsverarbeiter ist gem. Art. 4 Abs. 8 DSGVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

(3) Personenbezogene Daten sind gem. Art. 4 Abs. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „**Betroffener**“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

(4) Besonders schutzbedürftige personenbezogene Daten sind personenbezogenen Daten gem. Art. 9 DSGVO, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit von Betroffenen hervorgehen, personenbezogene Daten gem. Art. 10 DSGVO über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln sowie genetische Daten gem. Art. 4 Abs. 13 DSGVO, biometrischen Daten gem. Art. 4 Abs. 14 DSGVO, Gesundheitsdaten gem. Art. 4 Abs. 15 DSGVO sowie Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

(5) Verarbeitung ist gem. Art. 4 Abs. 2 DSGVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

(6) Aufsichtsbehörde ist gem. Art. 4 Abs. 21 DSGVO eine von einem Mitgliedstaat gem. Art. 51 DSGVO eingerichtete unabhängige staatliche Stelle.

§ 2 Vertragsgegenstand

(1) Der Auftragsverarbeiter erbringt für den Verantwortlichen die im Hauptvertrag genannten Leistungen. Dabei erhält der Auftragsverarbeiter Zugriff auf personenbezogene Daten, die der Auftragsverarbeiter für den Verantwortlichen ausschließlich im Auftrag und nach Weisung des Verantwortlichen verarbeitet. Die Datenverarbeitung erfolgt zu folgendem Zwecken:

- Zur Einrichtung eines Accounts
- Zur Nutzung von ContractHero zur Vertragsmanagement.

Der Umfang der Datenverarbeitung durch den Auftragsverarbeiter ergibt sich aus dem Hauptvertrag.

Dem Verantwortlichen obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung.

(2) Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrags vor.

(3) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei der der Auftragsverarbeiter und seine Beschäftigten oder durch den Auftragsverarbeiter Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Verantwortlichen stammen oder für den Verantwortlichen erhoben wurden.

(4) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüber hinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

§ 3 Weisungsrecht

(1) Der Auftragsverarbeiter darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Verantwortlichen erheben, verarbeiten oder nutzen; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird der Auftragsverarbeiter durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit.

(2) Die Weisungen des Verantwortlichen werden anfänglich durch diesen Vertrag festgelegt und können vom Verantwortlichen danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Verantwortliche ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten.

(3) Alle erteilten Weisungen sind vom Verantwortlichen zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

(4) Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung des Verantwortlichen gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Verantwortlichen unverzüglich darauf hinzuweisen. Der Auftragsverarbeiter ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Verantwortlichen bestätigt oder geändert wird. Der Auftragsverarbeiter darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

§ 4 Arten der verarbeiteten Daten, Kreis der Betroffenen

(1) Im Rahmen der Durchführung des Hauptvertrags erhält der Auftragsverarbeiter Zugriff auf die in **Anlage 1** näher spezifizierten personenbezogenen Daten.

(2) Der Kreis der von der Datenverarbeitung Betroffenen ist in **Anlage 2** dargestellt.

§ 5 Schutzmaßnahmen des Auftragsverarbeiters

(1) Der Auftragsverarbeiter ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Verantwortlichen erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

(2) Der Auftragsverarbeiter wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er hat die in **Anlage 3** genannten technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Verantwortlichen gem. Art. 32 DSGVO getroffen, die der Verantwortliche als angemessen anerkennt. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragsverarbeiter vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Den bei der Datenverarbeitung durch den Auftragsverarbeiter beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Der Auftragsverarbeiter wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (nachfolgend "**Mitarbeiter**"), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DSGVO) und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen.

(4) Der Auftragsverarbeiter hat einen Datenschutzbeauftragten benannt. Der Datenschutzbeauftragte des Auftragsverarbeiters ist heyData GmbH, Kantstr. 99, 10627 Berlin, datenschutz@heydata.eu, www.heydata.eu.

§ 6 Informationspflichten des Auftragsverarbeiters

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragsverarbeiters, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragsverarbeiter, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragsverarbeiter den Verantwortlichen unverzüglich informieren. Dasselbe gilt für Prüfungen des Auftragsverarbeiters durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;

b) eine Beschreibung der von dem Auftragsverarbeiter ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen;

c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten.

(2) Der Auftragsverarbeiter trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informiert hierüber den Verantwortlichen und ersucht um weitere Weisungen.

(3) Der Auftragsverarbeiter ist darüber hinaus verpflichtet, dem Verantwortlichen jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Absatz 1 betroffen sind.

(4) Über wesentliche Änderung der Sicherheitsmaßnahmen nach § 5 Abs. 2 hat der Auftragsverarbeiter den Verantwortlichen zu unterrichten.

§ 7 Kontrollrechte des Verantwortlichen

(1) Der Verantwortliche kann sich vor der Aufnahme der Datenverarbeitung und sodann jährlich von den technischen und organisatorischen Maßnahmen des Auftragsverarbeiters überzeugen. Hierfür kann er z. B. Auskünfte des Auftragsverarbeiters einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragsverarbeiters nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen oder durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragsverarbeiter steht. Der Verantwortliche wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragsverarbeiters dabei nicht unverhältnismäßig stören.

(2) Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf dessen mündliche oder schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragsverarbeiters erforderlich sind.

(3) Der Verantwortliche dokumentiert das Kontrollergebnis und teilt es dem Auftragsverarbeiter mit. Bei Fehlern oder Unregelmäßigkeiten, die der Verantwortliche insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragsverarbeiter unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Verantwortliche dem Auftragsverarbeiter die notwendigen Verfahrensänderungen unverzüglich mit.

§ 8 Einsatz von Dienstleister

(1) Die vertraglich vereinbarten Leistungen werden unter Einschaltung der in **Anlage 4** genannten Dienstleister (nachfolgend "**Unterauftragsverarbeiter**") durchgeführt. Der Verantwortliche erteilt dem Auftragsverarbeiter seine allgemeine Genehmigung im Sinne von Art. 28 Abs. 2 S. 1 DSGVO, im Rahmen seiner vertraglichen Verpflichtungen weitere Unterauftragsverarbeiter zu beauftragen oder bereits beauftragte zu ersetzen.

(2) Der Auftragsverarbeiter wird den Verantwortlichen vorab per E-Mail-Newsletter über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung eines Unterauftragsverarbeiters informieren. Der Verantwortliche kann gegen eine beabsichtigte Hinzuziehung oder die Ersetzung eines Unterauftragsverarbeiters aus wichtigem datenschutzrechtlichen Grund Einspruch erheben.

(3) Der Einspruch gegen die beabsichtigte Hinzuziehung oder die Ersetzung eines Unterauftragsverarbeiters ist innerhalb von 2 Wochen nach Versand der Information im E-Mail-Newsletter zu erheben. Wird kein Einspruch erhoben, gilt die Hinzuziehung oder Ersetzung als genehmigt. Liegt ein wichtiger datenschutzrechtlicher Grund vor und ist eine einvernehmliche Lösungsfindung zwischen dem Verantwortlichen und dem Auftragsverarbeiter nicht möglich, steht dem Verantwortlichen ein Sonderkündigungsrecht zum auf den Einspruch folgenden Monatsende zu.

(4) Der Auftragsverarbeiter hat bei der Einschaltung von Unterauftragsverarbeitern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten.

(5) Ein Unterauftragsverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragsverarbeiter Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragsverarbeiter für den Verantwortlichen erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Unterauftragsverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Verantwortlichen genutzt werden.

§ 9 Anfragen und Rechte Betroffener

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12–22 sowie 32 bis 36 DSGVO.

(2) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragsverarbeiter geltend, so reagiert dieser nicht selbstständig, sondern verweist den Betroffenen an den Verantwortlichen und wartet dessen Weisungen ab.

§ 10 Haftung

(1) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zum Auftragsverarbeiter alleine der Verantwortliche gegenüber dem Betroffenen verantwortlich.

(2) Der Auftragsverarbeiter haftet für Schäden unbeschränkt, soweit die Schadensursache auf einer vorsätzlichen oder grob fahrlässigen Pflichtverletzung des Auftragsverarbeiters, seines gesetzlichen Vertreters oder Erfüllungsgehilfen beruht.

(3) Für fahrlässiges Verhalten haftet der Auftragsverarbeiter nur bei Verletzung einer Pflicht, deren Erfüllung die ordnungsgemäße Durchführung des Vertrages überhaupt erst ermöglicht und auf deren Einhaltung der Verantwortliche regelmäßig vertraut und vertrauen darf, jedoch beschränkt auf den vertragstypischen Durchschnittsschaden. Im Übrigen ist die Haftung des Auftragsverarbeiters - auch für seine Erfüllungs- und Verrichtungsgehilfen - ausgeschlossen.

(4) Die Haftungsbegrenzung gemäß § 10.3 gilt nicht für Schadensersatzansprüche aus der Verletzung von Leben, Körper, Gesundheit oder aus der Übernahme einer Garantie.

§ 11 Beendigung des Hauptvertrags

(1) Der Auftragsverarbeiter wird dem Verantwortlichen nach Beendigung des Hauptvertrags alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder – auf Wunsch des Verantwortlichen, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragsverarbeiter. Der Auftragsverarbeiter hat den dokumentierten Nachweis der ordnungsgemäßen Löschung auf Anfrage zu führen.

(2) Der Verantwortliche hat das Recht, die vollständige und vertragsgerechte Rückgabe oder Löschung der Daten beim Auftragsverarbeiter in geeigneter Weise zu kontrollieren.

(3) Der Auftragsverarbeiter ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus solange gültig, wie der Auftragsverarbeiter über personenbezogene Daten verfügt, die ihm vom Verantwortlichen zugeleitet wurden oder die er für diesen erhoben hat.

§ 12 Schlussbestimmungen

(1) Soweit der Auftragsverarbeiters Unterstützungshandlungen nach dieser Vereinbarung nicht ausdrücklich kostenlos durchführt, kann er dem Verantwortlichen dafür eine angemessene Gebühr in Rechnung stellen, es sei denn, eigene Handlungen oder Unterlassungen des Auftragsverarbeiters haben diese Unterstützung unmittelbar erforderlich gemacht.

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Textform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

(3) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

(4) Diese Vereinbarung unterliegt deutschem Recht.

Verantwortlicher		**Auftragsverarbeiter**
Name:		Name: Sebastian Wengryn
Position:		Position: Gründer und CEO
Datum:		Datum:
Unterschrift:	Zweite Unterschrift:	Unterschrift:

Sebastian Wengryn

Anlagen

Anlage 1 – Beschreibung der Daten/Datenkategorien

- Personenstammdaten
- Kontakt-/Kommunikationsdaten (z. B. Telefon, Email)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten
- Produktdaten im Kundeneinsatz
- weitere Daten, die in über ContractHero verarbeiteten Dokumenten genannt sind

Anlage 2 – Beschreibung der Betroffenen/Betroffenengruppen

Verantwortlicher, Kunden des Verantwortlichen, Mitarbeiter des Verantwortlichen, andere Personen, die in über ContractHero verarbeiteten Dokumenten genannt sind

Anlage 3 – Technische und organisatorische Maßnahmen des Auftragsverarbeiters

1. Einleitung

Dieses Dokument fasst die von dem Auftragsverarbeiter getroffenen technische und organisatorischen Maßnahmen im Sinne von Art. 32 Abs. 1 DSGVO zusammen. Das sind Maßnahmen, mit denen der Auftragsverarbeiter personenbezogene Daten schützt. Das Dokument hat den Zweck, den Auftragsverarbeiter 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:

- Alarmanlage
- Automatisches Zugangskontrollsystem
- Chipkarten-/Transponder-Schließsystem
- Lichtschranken / Bewegungsmelder
- Manuelles Schließsystem (z.B. Schlüssel)
- Sicherheitsschlösser
- Videoüberwachung der Zugänge
- Klingelanlage mit Kamera
- Personenkontrolle beim Pförtner oder Empfang

- Schlüsselregelung / Schlüsselbuch
- Sorgfältige Auswahl von Sicherheitspersonal
- Tragepflicht von Mitarbeiter- und Gästeausweisen
- Besucher nur in Begleitung durch Mitarbeiter
- Arbeit im Home Office: Unbefugte haben kein Zutritt zur Wohnstätte der Mitarbeiter
- Arbeit im Home Office: Anweisung an Mitarbeiter, wenn möglich, in von Wohnräumen abgetrennten Arbeitszimmer zu arbeiten

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 Firewalls
- Einsatz von Mobile Device Management
- Einsatz von VPN-Technologie bei Remote-Zugriffen
- Verschlüsselung von Datenträgern
- Verschlüsselung von Smartphones
- BIOS-Schutz (separates Passwort)
- Automatische Desktopsperre
- Verschlüsselung von Notebooks / Tablets
- Verwaltung von Benutzerberechtigungen
- Zentrale Passwortregeln
- Nutzung von 2-Faktor-Authentifizierung
- Allgemeine Unternehmens-Richtlinie zum Datenschutz oder zur Sicherheit
- Unternehmens-Richtlinie für sichere Passwörter
- Unternehmens-Richtlinie "Löschen/Vernichten"
- Unternehms-Richtlinie "Cleandesk"
- Unternehmens-Richtlinie zur Verwendung mobiler Geräte
- Allgemeine Anweisung, bei Verlassen des Arbeitsplatzes Desktop manuell zu sperren

2.3. Zugriffskontrolle

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

- Vernichtung von Datenträgern mindestens nach DIN 66399 bzw. ISO/IEC 21964
- Physische Löschung von Datenträgern vor deren Wiederverwendung

- Protokollierung der Vernichtung von Daten
- 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
- Anweisung an Mitarbeiter, dass nur unbedingt erforderliche Daten ausgedruckt werden
- Anweisung an Mitarbeiter, dass Daten nur nach Rücksprache gelöscht werden

2.4. Trennungskontrolle

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

- Trennung von Produktiv- und Testsystem
- Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- Logische Mandantentrennung (softwareseitig)
- Bei pseudonymisierten Daten: Getrennte Aufbewahrung der Zuordnungsdatei auf einem getrennten, abgesicherten IT-System (möglichst verschlüsselt)
- Erstellung eines Berechtigungskonzepts
- Festlegung von Datenbankrechten
- Versehen der Datensätze mit Zweckattributen/Datenfeldern
- Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder nach Ablauf der gesetzlichen Löschfrist, wenn möglich, zu anonymisieren/pseudonymisieren.

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:

- Einrichtungen von VPN-Tunneln
- E-Mail-Verschlüsselung
- WLAN-Verschlüsselung (WPA2 mit starkem Passwort)
- Sichere Transportbehälter/-verpackungen
- Protokollierung von Zugriffen und Abrufen
- Bereitstellung von Daten über verschlüsselte Verbindungen wie SFTP oder HTTPS
- Nutzung von Signaturverfahren

- Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung oder der Löschfristen der Empfänger
- Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- Uploadverbot dienstlicher Daten auf unternehmensfremde Server

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
- Manuelle oder automatische Kontrolle der Protokolle
- Aufbewahrung von Formularen, deren Daten in automatisierte Verarbeitungen übernommen worden sind
- Erstellen einer Übersicht, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können
- 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
- Klare Zuständigkeiten für Löschungen
- Anweisung an Mitarbeiter, nur nach Rücksprache Daten zu löschen

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:

- Feuerlöschgeräte in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Klimaanlage in Serverräumen
- Schutzsteckdosenleisten in Serverräume
- Unterbrechungsfreie Stromversorgung (USV)
- Datenschutztresor
- Videoüberwachung in Serverräumen
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Regelmäßige Backups
- Erstellung eines Backup- & Recoverykonzepts

- Kontrolle des Sicherungsvorgangs
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
- Keine sanitären Anlagen im oder oberhalb des Serverraums
- Trennung von Betriebssystemen und Daten
- 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)

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
- Einsatz von Firewalls

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)
- Laufende Überprüfung von Auftragnehmern und ihren Tätigkeiten
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags, z.B. durch Anfrage entsprechender Bestätigungen

Anlage 4 – Aktuelle Subunternehmer

Name	**Funktion**	**Serverstandort**
Amazon Web Services EMEA SARL, Eschborner Landstraße 100, 60489 Frankfurt am Main, Deutschland	Bereitstellung der Server und Hostinginfrastruktur	EU
Twilio Inc., 375 Beale Street, Suite 300, San Francisco, CA 94105, USA	Versand von automatischen E-Mails aus der Anwendung, z.B. Einladungen, Erinnerungen und Benachrichtigungen an Nutzerinnen und Nutzer	EU
Google Ireland Ltd. (für Gemini), Gordon House, Barrow Street, Dublin 4, Irland	LLM (Verarbeitung von Textdateien zur Generierung von Antworten)	EU
Crisp IM, Boulevard de Launay, 44200 Nantes, Frankreich	Chatbot- und Live-Chat-Lösung	EU
Startdeliver AB, Klarabergsgatan 60, 111 21, Stockholm, Schweden	Plattform zur Verwaltung von Kundenbeziehungen	EU

Microsoft Azure, Microsoft Ireland Operations Ltd., One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland	Cloud-Computing-Dienste, Webanalyse (Heatmaps/ Sitzungsaufzeichnungen) und LLM-gestützte Textverarbeitung zur Generierung von Antworten	EU
Deepl SE, Maarweg 165, 50825 Köln, Deutschland	Online-Übersetzungsdienst, der auf künstlicher Intelligenz basiert	EU
Dropbox Inc., 333 Brannan Street, San Francisco, CA 94107 USA	Fortgeschrittene elektronische Signatur (FES)	EU
eID Easy OÜ, Telliskivi tn 60/1, Põhja-Tallinna linnaosa, 10412 Tallinn, Estland	Qualifizierte elektronische Signatur (QES)	EU
Modal Labs Inc., Offices in New York, San Francisco & Stockholm	Serverless Cloud-Computing Plattform für KI/ML-Workloads und Inferenz	EU
Qdrant Solutions GmbH, Chausseestraße 86, 10115 Berlin, Deutschland	Plattform für Vektor-Datenbank	EU