AUFTRAGSVERARBEITUNGS-VERTRAG

zwischen

ROTOP Pharmaka GmbH
eingetragen im Handelsregister des Amtsgerichts Dresden unter HRB 33711 und mit Geschäftsadresse in Bautzner Landstr. 400, 01328 Dresden

– nachfolgend ein "Verantwortlicher" und der "Erste Verantwortliche" –

und

Gemma Analytics GmbH
eingetragen im Handelsregister des Amtsgerichts Charlottenburg unter HRB 215822 B und mit Geschäfts-adresse in Chausseestraße 17, 10115 Berlin

– nachfolgend ein "Auftragsverarbeiter" und der "Erste Auftragsverarbeiter" –

– alle Verantwortlichen und Auftragsverarbeiter auch die "Parteien", einzeln jeweils eine "Partei".

ABSCHNITT I

Klausel 1 – Zweck und Anwendungsbereich

1. Mit diesem Auftragsverarbeitungs-vertrag (im Folgenden „AVV") soll die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr sichergestellt werden.
2. Die in Anhang I aufgeführten Verantwortlichen und Auftragsverarbeiter haben dem AVV zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 zu gewährleisten.
3. Der AVV gilt für die Verarbeitung personenbezogener Daten gemäß Anhang II.
4. Die Anhänge I bis IV sind Bestandteil des AVV.
5. Der AVV gilt unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 unterliegt.
6. Der AVV stellt für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 erfüllt werden.

Klausel 2 – Unabänderbarkeit der Klauseln

1. Die Parteien verpflichten sich, die Klauseln des AVV nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.
2. Dies hindert die Parteien nicht daran die in dem AVV festgelegten Klauseln in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

Klausel 3 – Auslegung

1. Werden in dem AVV die in der Verordnung (EU) 2016/679 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.
2. Der AVV ist im Lichte der Bestimmungen der Verordnung (EU) 2016/679 auszulegen.
3. Der AVV darf nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

Klausel 4 – Vorrang

Im Falle eines Widerspruchs zwischen dem AVV und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben der AVV Vorrang.

Klausel 5 – Kopplungsklausel

1. Eine Einrichtung, die nicht Partei des AVV ist, kann dem AVV mit Zustimmung aller Parteien jederzeit als Verantwortlicher oder als Auftragsverarbeiter beitreten, indem sie die Anhänge ausfüllt und Anhang I unterzeichnet.

2. Nach Ausfüllen und Unterzeichnen der unter Nummer 1 genannten Anhänge wird die beitretende Einrichtung als Partei des AVV behandelt und hat die Rechte und Pflichten eines Verantwortlichen oder eines Auftragsverarbeiters entsprechend ihrer Bezeichnung in Anhang I.
3. Für die beitretende Einrichtung gelten für den Zeitraum vor ihrem Beitritt als Partei keine aus dem AVV resultierenden Rechte oder Pflichten.

ABSCHNITT II – PFLICHTEN DER PARTEIEN

Klausel 6 – Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in Anhang II aufgeführt.

Klausel 7 – Pflichten der Parteien

7.1 Weisungen

1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf angemessen dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.
2. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

7.2 Zweckbindung

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Anhang II genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

7.3 Dauer der Verarbeitung personenbezogener Daten

Die Daten werden vom Auftragsverarbeiter nur für die in Anhang II angegebene Dauer verarbeitet.

7.4 Sicherheit der Verarbeitung

1. Der Auftragsverarbeiter ergreift mindestens die in Anhang III aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten"). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.
2. Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung

des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7.5 Sensible Daten

Falls die Verarbeitung personenbezogene Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten"), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

7.6 Dokumentation und Einhaltung des AVV

1. Die Parteien müssen die Einhaltung des AVV nachweisen können.
2. Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß des AVV umgehend und in angemessener Weise.
3. Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in dem AVV festgelegten und unmittelbar aus der Verordnung (EU) 2016/679 hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diesen AVV fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.
4. Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.
5. Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

7.7 Einsatz von Unterauftragsverarbeitern

1. Der Auftragsverarbeiter darf keinen seiner Verarbeitungsvorgänge, die er im Auftrag des Verantwortlichen gemäß des AVV durchführt, ohne vorherige gesonderte schriftliche Genehmigung des Verantwortlichen an einen Unterauftragsverarbeiter untervergeben. Der Auftragsverarbeiter reicht den Antrag auf die gesonderte Genehmigung mindestens 5 Tage vor der Beauftragung des betreffenden Unterauftragsverarbeiters zusammen mit den Informationen ein, die der Verantwortliche benötigt, um über die Genehmigung zu entscheiden. Die Liste der vom Verantwortlichen genehmigten Unterauftragsverarbeiter findet sich in Anhang IV. Die Parteien halten Anhang IV jeweils auf dem neuesten Stand.
2. Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß des AVV gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend des AVV und gemäß der Verordnung (EU) 2016/679 unterliegt.
3. Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener

Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

4. Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.
5. Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche – im Falle, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

7.8 Internationale Datenübermittlungen

1. Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 im Einklang stehen.
2. Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 7.7 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

Klausel 8 – Unterstützung des Verantwortlichen

1. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.
2. Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Nummern 1 und 2 befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.
3. Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 8 Nummer 2 zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:
    1. Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung"), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;
    2. Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;

3. Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;
4. Verpflichtungen gemäß Artikel 32 der Verordnung (EU) 2016/679.

4. Die Parteien legen in Anhang III die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der Anwendung dieser Klausel 8 sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

Klausel 9 – Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

9.1 Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

1. bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);
2. bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der Verordnung (EU) 2016/679 in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:
    1. die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
    2. die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
    3. die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt;

1. bei der Einhaltung der Pflicht gemäß Artikel 34 der Verordnung (EU) 2016/679 die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

9.2 Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

1. eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);
2. Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;
3. die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

Die Parteien legen in Anhang III alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Artikel 33 und 34 der Verordnung (EU) 2016/679 zu unterstützen.

ABSCHNITT III – SCHLUSSBESTIMMUNGEN

Klausel 10 – Verstöße gegen den AVV und Beendigung des Vertrags

1. Falls der Auftragsverarbeiter seinen Pflichten gemäß des AVV nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er den AVV einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, den AVV einzuhalten.
2. Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß des AVV betrifft, wenn
    1. der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Nummer 1 ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;
    2. der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen den AVV verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 nicht erfüllt;
    3. der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß des AVV, der Verordnung (EU) 2016/679 zum Gegenstand hat, nicht nachkommt.
3. Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß des AVV betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 7.1 Nummer 2 verstoßen.
4. Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung des AVV.

ANHANG I: LISTE DER PARTEIEN

Erster Verantwortlicher

Ort, Datum

Verantwortlicher
Vertreten durch:
Dr. Michael Peterseim
CFO

Erster Auftragsverarbeiter

Ort, Datum

Auftragsverarbeiter
Vertreten durch:
Bijan Soltani
Geschäftsführer
bijan.soltani@gemmaanalytics.com

Datenschutzbeauftragter des Ersten Auftragsverarbeiters:
heyData GmbH
Schützenstr. 5
10117 Berlin
datenschutz@heydata.eu
www.heydata.eu

ANHANG II: BESCHREIBUNG DER VERARBEITUNG

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden

- Kunden / Interessenten / Nutzer des Verantwortlichen
- Mitarbeiter des Verantwortlichen
- Lieferanten des Verantwortlichen

Kategorien personenbezogener Daten, die verarbeitet werden

- Bestandsdaten (z. B. Namen, Adressen)
- Kontaktdaten (z. B. E-Mail, Telefonnummern)
- Inhaltsdaten (z. B. Texteingaben, Fotos, Videos)
- Vertragsdaten (z. B. Vertragsgegenstand, Laufzeit)
- Zahlungsdaten (z. B. Bankverbindung, Zahlungshistorie)
- Nutzungsdaten (z. B. Interessen, besuchte Websites, Kaufverhalten, Zugriffszeiten, Protokolldaten)
- Meta-/Kommunikationsdaten (z. B. Geräte-IDs, IP-Adressen, Standortdaten)
- Mitarbeiterstammdaten (z. B. Namen, Adressen, Lohngruppe, Steuermerkmale)
- Bewerberdaten (z. B. Namen, Kontaktdaten, Qualifikationen, Bewerbungsunterlagen)

Art der Verarbeitung

- Einsichtnahme, temporäre Speicherung und Verarbeitung personenbezogener Daten in lokalen oder projektbezogenen Entwicklungs- und Testumgebungen des Auftragsverarbeiters, soweit dies zur Analyse oder technischen Umsetzung erforderlich ist.
- Modellierung, Transformation und Qualitätssicherung von Daten im Rahmen von Entwicklungs- und Implementierungsleistungen (z. B. Datenmodellierung, Pipeline-Logiken, Tests).
- Analyse und Auswertung von Daten zur Identifikation fachlicher Anforderungen, zur Validierung von Ergebnissen sowie zur Vorbereitung und Erstellung von Berichten und Dashboards.
- Konfiguration und Implementierung von Entwicklungsartefakten (z. B. ELT-Prozesse, dbt-Projekte, Airflow-DAGs, Schnittstellen).
- Fehleranalyse, Debugging und technische Tests.
- Beratungs- und Unterstützungsleistungen im Bereich Datenplattformen, Datenmodelle und Analytics-Architekturen, soweit hierfür eine Verarbeitung personenbezogener Daten erforderlich ist.

Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden

- Speicherplatz (Webhosting)
- Software als Dienstleistung (Rechenkapazität, Datenbanken, Software)
- Telekommunikationsdienste (E-Mails)
- Domain-Registrierung
- Software- und Designentwicklung/Beratung oder Wartung
- Serveradministration/Hardwarewartung
- Datenanalyse/Beratungsdienstleistungen
- Werbung/Marketing

Dauer der Verarbeitung

Die Dauer der Verarbeitung entspricht der Dauer des entsprechenden Vertrags zwischen den Parteien.

ANHANG III: TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN EINSCHLIESSLICH ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN

Beschreibung der von dem/den Verantwortlichen ergriffenen technischen und organisatorischen Sicherheitsmaßnahmen (einschließlich aller relevanten Zertifizierungen) zur Gewährleistung eines angemessenen Schutzniveaus unter Berücksichtigung der Art, des Umfangs, der Umstände und des Zwecks der Verarbeitung sowie der Risiken für die Rechte und Freiheiten natürlicher Personen:

Maßnahme	**Beschreibung**
Zugangskontrolle	Alle Eingänge sind angemessen gegen unbefugten Zugang gesichert, was bedeutet, dass: Außentüren mit manuellen Schlössern gesichert sind; Besucher dürfen die Räumlichkeiten nur in Begleitung eines Mitarbeiters betreten; Drittpersonen werden sorgfältig ausgewählt, insbesondere für Reinigungs- und Wartungsarbeiten; Bei der Arbeit im Homeoffice: Die Mitarbeiter werden angewiesen, nach Möglichkeit in einem vom Wohnbereich getrennten Raum zu arbeiten.
Organisatorische Datenschutzmaßnahmen	Organisatorische Maßnahmen: Es finden regelmäßig Schulungen zum Thema Datenschutz statt. Regelmäßige Sensibilisierung der Mitarbeiter. Es wurde eine Clean-Desk-Policy definiert. Die Anzahl der Administratoren ist auf das erforderliche Minimum beschränkt. Allgemeine Verpflichtung zur Vermeidung von Papier. Personenbezogene Daten werden in der Regel nicht ausgedruckt, sondern überwiegend digital verarbeitet. Die Mitarbeiter sind außerdem angewiesen, nur absolut notwendige Daten auszudrucken. Interne Anweisung, personenbezogene Daten bei Offenlegung oder nach Ablauf der gesetzlichen Löschfrist nach Möglichkeit zu anonymisieren/pseudonymisieren.
Kontrolle der Übermittlung	Die Aspekte der Übermittlung personenbezogener Daten werden umgesetzt durch: Verschlüsselung von Datenträgern und Verbindungen; WLAN-Verschlüsselung über WPA2 mit starkem Passwort; Bei physischen Transporten werden geeignete Transportpersonen sorgfältig ausgewählt.
Datenschutzmanagement	Die folgenden Maßnahmen sollen sicherstellen, dass die Organisation die grundlegenden Anforderungen des Datenschutzrechts erfüllt:

	Nutzung der heyData-Plattform für das Datenschutz-management; Ernennung des Datenschutzbeauftragten heyData; Verpflichtung der Mitarbeiter zur Geheimhaltung von Daten; Regelmäßige Schulung der Mitarbeiter zum Thema Datenschutz; Führung einer Übersicht über die Verarbeitungsvor-gänge (Art. 30 DSGVO).
Incident Response Management	Die folgenden Maßnahmen sollen sicherstellen, dass bei Datenschutzverletzungen Meldeprozesse ausge-löst werden: Meldeverfahren für Datenschutzverletzungen gemäß Art. 4 Nr. 12 DSGVO an die Aufsichtsbehörden (Art. 33 DSGVO); Benachrichtigungsprozess bei Datenschutzverletzun-gen gemäß Art. 4 Nr. 12 DSGVO gegenüber den betrof-fenen Personen (Art. 34 DSGVO); Einbeziehung des Datenschutzbeauftragten bei Si-cherheitsvorfällen und Datenschutzverletzungen.
Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)	Die folgenden umgesetzten Maßnahmen berücksich-tigen die Anforderungen der Grundsätze „Privacy by Design“ und „Privacy by Default“: Schulung der Mitarbeiter in „Privacy by Design“ und „Privacy by Default“; Es werden nicht mehr personenbezogene Daten erho-ben, als für den jeweiligen Zweck erforderlich sind.
Eingabekontrolle	Die Kontrolle der Eingaben erfolgt durch: Protokollierung von Dateneingaben, Änderungen und Löschungen mit manueller oder automatischer Kon-trolle der Protokolle; Zugriffsrechte (sowohl für Benutzer als auch für Admi-nistratoren) basieren auf den Anforderungen der Auf-gabe und dem Datenschutzgesetz.
Auftragskontrolle	Die Vergabe und Überwachung von Auftragsdatenver-arbeitungen erfolgt auf Grundlage folgender Kriterien: Auswahl der Auftragnehmer unter Due-Diligence-Aspekten; detaillierte Regelungen zum Vertragsverhältnis; schriftliche Anweisungen an den Auftragnehmer oder Anweisungen in Textform (z. B. durch einen Auftrags-verarbeitungs-vertrag); Sicherstellung, dass die Daten nach Abschluss des Auf-trags vernichtet werden, z. B. durch Einholung entspre-chender Bestätigungen; Bestätigung der Auftragnehmer, dass sie ihre eigenen

	Mitarbeiter zur Geheimhaltung der Daten verpflichten (in der Regel im Auftragsverarbeitungs-vertrag); Vereinbarung über Kontroll- und Zugriffs- oder Löschungsrechte.

ANHANG IV: LISTE DER UNTERAUFTRAGSVERARBEITER

Der Verantwortliche hat folgende Unterauftragsverarbeiter genehmigt:

Name des Unterauftragsverarbeiters	**Adresse**	**Art der Verarbeitung v. Daten**	**Internationaler Transfer (falls zutreffend)**
Langdock GmbH	Greifswalder Str. 212, 10405 Berlin, Deutschland	KI-gestützte Workflows, Dokumentenverarbeitung und allgemeine LLM-Nutzung (nur EU-gehostete Modelle)	Keiner
Amazon Web Services EMEA SARL	38 Avenue John F. Kennedy, L-1855 Luxemburg, Luxemburg	Cloud-Computing und KI-Modell-Hosting (AWS Bedrock, Region Frankfurt)	Keiner
Google Ireland Limited	Gordon House, Barrow Street, Dublin 4, Irland	Cloud-Speicher (Google Drive) und KI-gestützte Meeting-Zusammenfassungen (Gemini)	Keiner
Anthropic, PBC	548 Market St, PMB 90375, San Francisco, CA 94104, USA	KI-gestützte Softwareentwicklung und Codegenerierung (Claude)	USA, EU-SCCs
Mango Technologies, Inc. (dba ClickUp)	350 10th Ave, Suite 500, San Diego, CA 92101, USA	Projektmanagement und Aufgabenverwaltung	USA, EU-SCCs
Notion Labs, Inc.	2300 Harrison Street, San Francisco, CA 94110, USA	Projektmanagement, Aufgabenverwaltung, Dokumentation und Wissensmanagement	USA, EU-SCCs
Fireflies.AI Corp.	5424 Sunol Blvd, Ste 10-531, Pleasanton, CA 94566, USA	Meeting-Transkription und automatisierte Notizen	USA, EU-SCCs